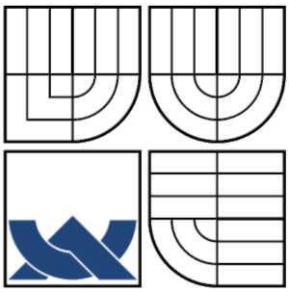
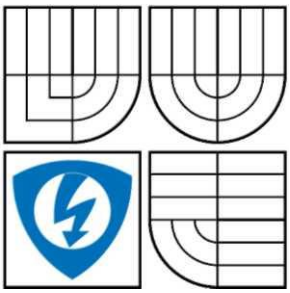


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ZAJIŠTĚNÍ QOS V BEZDRÁTOVÝCH SÍTÍCH

QOS ASSURANCE IN WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE

BACHELOR´S THESIS

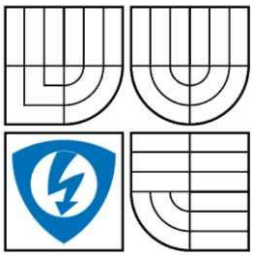
AUTOR PRÁCE — FILIP DVOŘÁK

AUTHOR

VEDOUCÍ PRÁCE — Ing. MICHAL VYMAZAL

SUPERVISOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student: Filip Dvořák ***ID:*** 47235
Ročník: 3. ***Akademický rok:*** 2009/2010

NÁZEV TÉMATU:

Zajištění QoS v bezdrátových sítích

POKYNY PRO VYPRACOVÁNÍ:

Popište a definujte parametry a využitelnost zajištění kvality služeb (QoS) v bezdrátových sítích. Podrobně popište standard 802.11e a principy realizace lokální sítě WiFi s připojením k Internetu. Seznamte se simulačním prostředím Opnet Modeler. V tomto prostředí vytvořte bezdrátovou lokální síť, ve které nakonfigurujte mechanizmus pro zajištění kvality služeb pro přenos dat citlivých na zpoždění (IP telefony, přenos videa, hlasu a multimédií obecné) a následně proveďte podrobnou analýzu hlavních sítových QoS statistik. Výsledky analýzy prezentujte formou grafu a tabulek. Závěrem zhodnoťte význam QoS mechanizmu v bezdrátových sítích.

DOPORUČENÁ LITERATURA:

[1] Zandl, P: Bezdrátové sítě Wi-Fi, Computer Press, 2003, ISBN: 807226632.
[2] Brisbon, S.: Wi-Fi - postavte si svou vlastní Wi-Fi síť, Neokortex, 2004, ISBN 80-86330-13-3

Termín zadání: 29.1.2010 ***Termín odevzdání:*** 2.6.2010

Vedoucí práce: Ing. Michal Vymazal

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Anotace

Bakalářská práce pojednává o bezdrátových sítích WiFi, popisuje základní standardy a jejich doplňky. Práce je rozdělena na 2 části – teoretickou a praktickou. První část je věnována teoretickému popisu nejznámějších standardů IEEE 802.11 a detailnímu popisu standardu 802.11e. Druhá část práce se zabývá návrhem a vlivem služby Wireless Multimedia v bezdrátové síti jak v reálném prostředí, tak i v simulačním programu Opnet Modeler. V závěru jsou shrnuty a popsány získané výsledky měření.

The Abstract

The bachelor´s work deals with wireless network WiFi and describes basic standards and their supplements. This work is divided into two parts - theoretical and practical. The first part of the work is applied to theoretic description of the best known standards IEEE 802.11 and detailed description of standard 802.11e. The second part of the work takes an interest in proposal and influence of service Wireless Multimedia in wireless network both in real world and in simulation program Opnet Modeler. Obtained results of the measurement are described and summarized in the conclusion.

Klíčová slova

WiFi, 802.11e, QoS, WMM, OPNET Modeler, VoIP

Keywords

WiFi, 802.11e, QoS, WMM, OPNET Modeler, VoIP

Bibliografická citace

DVOŘÁK, F. *Zajištění QoS v bezdrátových sítích*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2010. 89 s. Vedoucí bakalářské práce Ing. Michal Vymazal.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma **Zajištění QoS v bezdrátových sítích** jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury v závěru práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne……. …….

podpis autora

Poděkování

Chtěl bych poděkovat Ing. Michalu Vymazalovi za zodpovídání mých dotazů a vedení mé bakalářské práce. Dále firmě NWT Computer za zapůjčení vybavení a panu Stanislavu Žaludovi za umožnění přístupu do areálu školy Acorn's & John's school s.r.o. V neposlední řadě i Mgr. Adéle Dohnalové za pomoc při korekci této práce.

V Brně dne …… ……

Podpis

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Bezdrátové sítě jsou v dnešní době rozšířeny v takovém množství, že se s nimi setkáváme prakticky na každém kroku. Každý den je používáme k získávání informací, výměně dat nebo ke komunikaci s dalšími účastníky. V této práci se budu zabývat bezdrátovými sítěmi (WiFi - *Wireless Fidelity)* sloužícími jako rychlé a levné spojení s internetem.

Sítě WiFi vznikly jednak jako levné řešení „poslední míle“ nebo také k vytvoření sítě v místech, kde bylo složité řešit spojení pevnou kabeláží, a to buď z finančních či stavebních důvodů (např. historické budovy apod.). Postupem času se však v sítích WiFi začaly objevovat služby, na které nebyly tyto sítě navrhované. Jedná se například o VoIP (*Voice over IP*- přesněji VoWLAN), proudové vysílání videa a další typy multimediálních služeb. Tyto služby potřebují ke svému bezproblémovému provozu určitou garanci některých parametrů ze strany sítě. Jedná se hlavně o zpoždění, kolísání zpoždění (*jitter*), ztrátovost paketů a šířku pásma. Sítě WiFi ve svém původním návrhu nemohly vyhovět nárokům jednotlivých aplikací. Než je totiž přistoupeno k samotnému vyslání dat, musí stanice překonat řadu kroků a časových mezer. Při neexistenci priorit tak stanice s daty přistupují k médiu náhodně. Žádná garance parametrů tedy nepřipadá v úvahu. Při rostoucí zátěži se požadavky na vysílání mezi stanicemi mohou střetnout - vznikají kolize. Doba, než jsou data vyslána, se tak může několikanásobně prodloužit.

V roce 2005 byl dokončen mechanismus, který umožnil bezproblémové využití multimediálních služeb v sítích WiFi. Standard 802.11, jež doplňuje existující standardy třídy 802.1, přináší nové techniky přístupu k médiu, které umožňují upřednostňování paketů na základě rozdělení do několika priorit a tříd provozu. O tomto standardu a službě Wireless Multimedia bude pojednávat i druhá část bakalářské práce.

Na závěr je popsáno vytvoření a realizace bezdrátové sítě s podporou 802.11e v simulačním programu OPNET Modeler.

Cílem této práce je ukázat přínos služby Wireless Multimedia v bezdrátové síti a přinést čtenáři ucelený souhrn informací o těchto sítích a reálném uplatnění služeb založených na mechanismu QoS.

2 Bezdrátové sítě

Bezdrátovými sítěmi jsou myšleny všechny sítě, ve kterých se můžeme volně pohybovat v místech dosahu vysílače a jejich přenosovým médiem je rádiové prostředí. Výhoda oproti klasickým kabelovým sítím je zde určitá mobilita účastníků. Jako nevýhodu je možno považovat to, že signál je šířen ve specifickém přenosovém prostředí a může být tedy ovlivněn řadou faktorů, např. rušením od ostatních bezdrátových sítí nebo útlumem způsobeným odrazem od překážek.

Aktuálním problémem těchto sítí je zajištění bezpečnosti. Signál je přenášen „vzduchem“, a proto je velmi složité bezpečně vymezit prostor, kde má být síť dostupná, a kde již ne. K datům se může dostat prakticky kdokoliv, kdo má potřebné vybavení a samozřejmě i potřebné znalosti. Aby se neoprávněným průnikům zabránilo je nutno zavést šifrování dat s některou z dalších forem ochrany. Více viz kapitola 2.1.5.

Bezdrátové sítě můžeme rozdělit podle několika kritérií (např. podle šířky pásma, mobility apod.). Pro tuto práci bylo zvoleno dělení dle typu signálů. [16]

Rádiové sítě patří k nejběžnějším sítím, se kterými se můžeme setkat (např. GSM - *Global System for Mobile communications*). Rádiové sítě mají rozsah od několika metrů, až po desítky kilometrů. Pro přenos se používá rádiových vln různých kmitočtů (např. v síti GSM - 900 nebo 1800 MHz).

Infračervené sítě jsou určeny pro přenos informací jen na malé vzdálenosti v řádu jednotek metrů. Dříve byly v mobilních telefonech, PDA nebo v přenosných počítačích, dnes je již nahrazujeme technologií Bluetooth. Pro přenos se využívá světelného paprsku o vlnové délce 875 nm. Určitou nevýhodou je nutnost přímé viditelnosti mezi zařízeními. Naopak podstatnou výhodou je velká šířka pásma (byly testovány rychlosti až stovky Mbit/s), a také fakt, že jejich licenční pásmo není nijak limitováno. To je zřejmé z jejich vlastností, malého dosahu a potřeby přímé viditelnosti, protože frekvence používaná sítí v jednom místě může být znovu použita jen o několik metrů dál. [23]

Optické bezdrátové sítě - bezdrátová optika FSO (*Free Space Optics*) - je technologie pracující na stejném principu jako optické vlákno, s tím rozdílem, že přenosovým médiem je atmosféra. Využívá se přenosových rychlostí od 100 Mbit/s až do 2,5 Gbit/s. Pro přenos vzduchem se používá světlo o několika vlnových délkách -

dlouhé vlny 1550 nm (194 THz) a krátké vlny 800 nm (375 THz). Tyto signály patří do oblasti infračerveného spektra. Požadavkem na přenos je přímá viditelnost. Výhodou je relativní bezpečnost. Útočník by musel zachytit velmi tenký paprsek, který je velmi často vysoko nad zemí.

Obrázek 2-1 Zařízení firmy Lightpointe pro FSO

Na Obrázku 2-1 je zařízení od firmy Lightpointe, které umožňuje dosáhnout rychlosti až 1,25 Gbit/s na vzdálenost 1km.

2.1 Standardy 802.11

S postupem času je standard 802.11 rozšiřován a zrychlován řadou doplňujících standardů, které z hlavní části vytváří organizace IEEE (*Institute of Electrical and Electronics Engineers*). Jednotná tvorba je důležitá pro standardizaci jednotlivých norem a kompatibilitu výrobků. Zde budou popsány jen některé z nich. [14] [16] [23]

2.1.1 802.11a (IEEE 1999)

Standard 802.11a pracuje na frekvenci 5,1 – 5,3 a 5,725 – 5,825 GHz. Podporuje mechanismus přenosu OFDM (*Orthogonal Frequency Division Multiplex*) a umožňuje dosáhnout rychlosti až 54 Mbit/s (v praxi okolo 36 Mbit/s – režie provozu, šifrování, rušení apod.). Vysílací výkon je 40 – 800 mW. Za výhodu je možno považovat pracovní pásmo 5 GHz. V pásmu 5 GHz je menší rušení od okolních vlivů, a tak lze u tohoto pásma využívat více nepřekrývajících se kmitočtů.

Tento standard se u nás příliš nerozšířil. Hlavní důvody jsou pořizovací náklady a blokování pásma 5 GHz evropskou organizací ETSI (*European Telecommunication Standards Institute*) z důvodu přípravy pro sítě HiPerLan (*High Performance LAN*),

které pracují na podobných frekvencích jako 802.11a - 5,15 až 5,30 GHz. Přizpůsobení 802.11a pro Evropu je řešeno v standardu 802.11h, jenž je doplňkem 802.11a a jsou v ní obsaženy nové funkce DFS (*Dynamic Frequency Selection*) a TPC (*Transmit Power Control*). DFS je dynamické přidělování nejméně rušené a zatížené frekvence stanicím. TPC řídí a reguluje vysílací výkon tak, aby se minimalizovalo rušení ostatních sítí.

2.1.2 802.11b (IEEE 1999)

Používá techniku DSSS (*Direct Sequence Spread Spectrum*) s CCK (*Complementary Code Keying*), a tak nabízí maximální rychlost až 11 Mbit/s. Reálná rychlost se ale pohybuje okolo 6 Mbit/s, protože 30 až 40% pásma je použito na režii při provozu. Vysílací výkon je omezen až do úrovně 200mW. Dnes je tato norma nahrazena rychlejší 802.11g.

Podporuje několik druhů rychlostí – 11; 5,5; 2; 1 Mbit/s. Rychlost je snižována v závislosti na rušení sítě na takovou úroveň, aby byla zachována nízká chybovost a ztrátovost paketů.

2.1.3 802.11g (IEEE 2003)

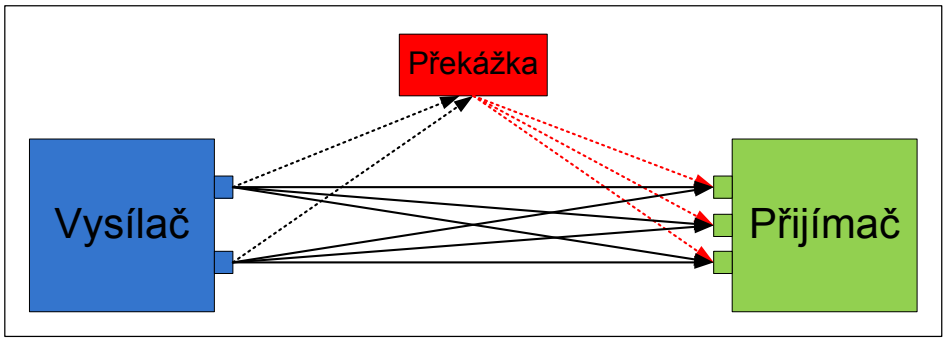
Nejrozšířenější norma, která dnes pomalu ustupuje rychlejší 802.11n. Používá přenosovou techniku pracující s tzv. rozprostřeným spektrem OFDM (*Orthogonal Frequency Division Multiplexing)* a podporuje rychlosti 54; 48; 36; 24 Mbit/s (modulace 16-QAM *Quadrature amplitude modulation*), 18 a 12 Mbit/s (QPSK-*Quadrature Phase-Shifi Keying*), 9 a 6 Mbit/s (BPSK *Binary Phase-Shifi Keying*). Nižší rychlosti používají techniku DSSS (*Direct Sequence Spread Spectrum*) z důvodu zpětné kompatibility s normou 802.11b – 11; 5,5; 2; 1 Mbit/s. Kdyby tomu tak nebylo, zařízení normy 802.11b by bralo OFDM signál pouze jako šum. Rychlost v praxi je při vynikajícím signálu a přijatelné vzdálenosti asi 30 Mbit/s (režie je cca 30 – 40%).

Je zaručena i zpětná kompatibilita s normou 802.11b. Ale při připojení stanice využívající pomalejší normy klesá rychlost v celé síti 802.11g z důvodu použití mechanismu posílání rámců RTS/CTS. Pomalejší stanice musí požádat přístupový bod (*Access point* - dále jen AP) o povolení vysílat, a tím i zablokovat médium pro svůj přenos. Díky tomuto principu se zamezí současnému vysílání klientů 802.11b, g.

2.1.4 802.11n (IEEE 2009)

Udávaná maximální rychlost na fyzické vrstvě je 600 Mbit/s, avšak rychlost v praxi se pohybuje okolo 200 Mbit/s. Tak vysoké rychlosti je dosaženo využitím několika způsobů - technologií MIMO (*Multiple-Input Multiple-Output*), rozšíření šířky kanálu na 40MHz jejich sdružováním, spojování rámců (*frame aggregation*), block ACK (*Acknowledge*), a také využíváním OFDM.

MIMO – hlavní předností této technologie je možnost vyslání více nezávislých signálů různými cestami a anténami v jednom frekvenčním kanále, čímž se sníží chybovost signálu a zvýší kapacita – prostorový multiplex (*Spatial Multiplexing*). Jednotlivé cesty jsou voleny v závislosti na kvalitě přijatého signálu (vysoká hodnota odstupu signál/šum - SNR). Využívá se odrazů signálu od pevných překážek, a tím i různě dlouhých cest signálu k přijímači. U 802.11b, g tato skutečnost byla brána jako rušení - vícecestné interference, kdy signál přišel s různým zpožděním v závislosti na délce cesty a výsledný signál byl po složení deformovaný. Přijímač pak, podle určitých algoritmů a různých signatur vysílaných jednotlivými anténami, vyhodnotí přijaté signály a správně je seřadí. Používán je i mechanismus formování vysílaného signálu (*beamforming*), kdy je měněna fáze vyslaného signálu v závislosti na vzdálenosti tak, aby signál v přijímači měl co možná největší hodnotu SNR. Dnes jsou využívány až 4 antény uvnitř a 16 vně budovy.



Obrázek 2-2 Vícecestné šíření signálu [6]

Frame aggregation – v normě 802.11b, g se na zátěži a zpoždění výrazně projevuje čekání při přenosu, např. časový interval mezi rámci (DIFS - *DCF InterFrame Space*) nebo náhodné čekací doby při „soutěžení“ o médium při kolizích. U 802.11n je využito shlukování rámců na MAC podvrstvě. Zmenšuje se tak čekání mezi rámci, a také se může zrychlovat potvrzování rámců tím, že potvrzovací rámec ACK bude vyslán až po

vyslané sekvenci rámců - (*block Acknowledge*). Tímto způsobem lze snížit režii až na 25%. V případě, kdy se bude rušení nebo chybovost zvětšovat, budou použity standardní metody přenosu. [6] [18] [20]

2.1.5 802.11i (IEEE 2004)

Při návrhu 802.11 byl vytvořen zabezpečovací mechanismus WEP (*Wired Equivalent Privacy*). Ten měl za úkol šifrovat komunikaci a zajistit bezpečnou autentizaci klientské stanice k AP. Postupem času však došlo k prolomení této ochrany. Dnes již může útočník zjistit WEP klíč pouhým monitorováním sítě a využitím některého z volně dostupného softwaru (např. Aircrack [soubor programů] pod Linuxem) k zachycení potřebného množství paketů, a tím i k získání dynamického vektoru IV (*Initialization Vector*). Vzhledem k tomu, že bakalářská práce není na téma „bezpečnost" primárně zaměřena, je popis této oblasti pouze zjednodušený.

Tento pasivní útok je založen na principu fungování celého mechanismu. WEP nabízí v nejslabší verzi 64 bitový klíč. Někteří výrobci jej však rozšířili až na 128 nebo 256 bitový. Tento klíč je tvořen ze sdíleného klíče o délce 40 bitů, sloužícího k ověřování stanic při připojování k AP a 24 bitového vektoru IV.

K **šifrování** přenosu dat se využívá celé délky klíče – 40 bit + 24 bit IV. Tento klíč je rozšířen na délku zprávy pomocí generátoru pseudonáhodných čísel, řízeným podle nastavených pravidel (ty jsou dány použitou šifrou RC4 - proudová šifra, kde šifrování probíhá po bajtech), které musí znát oba účastníci. Poté je provedena operace XOR (*exkluzivní logický součet*) s daty, které budou vyslány. Ještě než jsou data odeslána, je před ně vložen vektor IV (v něm je přenášena zmíněná „pseudonáhodnost").

Postup **dešifrování** je následující - stanice přijme data, oddělí z nich vektor IV, jež je následně připojen ke sdílenému klíči. Tento klíč je opět zvětšen na délku dat a je provedena operace XOR. Tím se získají nezašifrovaná data. Pro zvýšení bezpečnosti je IV generován pro každý paket zvlášť.

Jak již bylo zmíněno výše, existuje řada programů na monitorování paketů ve WiFi sítích. Ty odchytávají pakety a v nich umístěné IV a po určitém množství jsou schopny získat sdílený klíč. Udává se, že programu AirCrack stačí k prolomení 64 bit klíče získat okolo 300 000 IV. [19] [23]

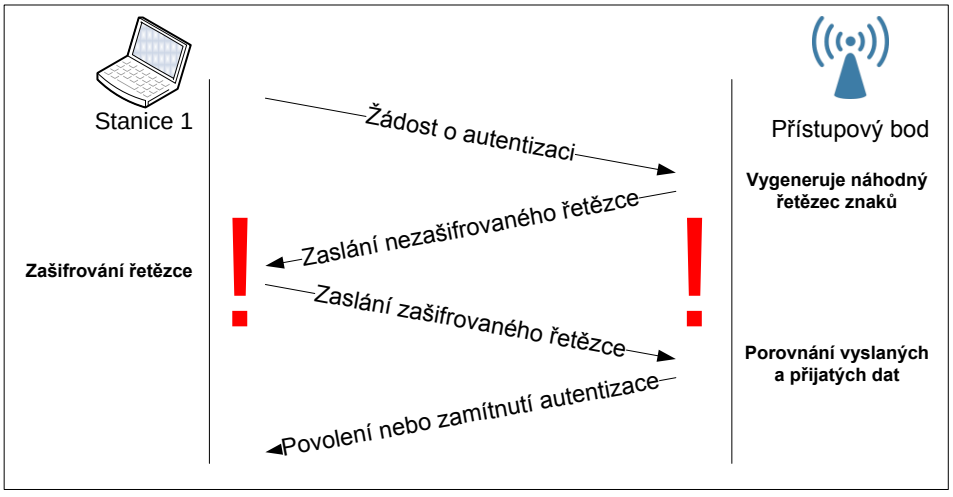
Nevýhody WEP:

- vektor IV se přenáší nezašifrovaně, začíná se opakovat po 2^{24} kombinacích
- WEP neřeší distribuci klíče – musí se zadávat na všech stanicích ručně (bez podpory 802.11x); klíč je možno získat fyzickou krádeží samotného zařízení
- jednostranná autentizace – AP nemusí stanicím prokazovat svou totožnost

I přes jeho nevýhody je často využíván, a to z několika důvodů. Prvním je používání směrovačů s továrním nastavením - využívají WEP spolu s veřejně známými hesly pro přístup. Dalším důvodem je myšlení některých uživatelů, kteří jsou přesvědčení, že do jejich „domácí" sítě s přístupem na internet a se sdílenými daty nemá nikdo chuť proniknout. Při malém pokus bylo objeveno celkem 22 WiFi sítí z nichž 12 používalo šifrování WPA nebo WPA2, 7 používalo WEP a 3 byly zcela otevřené.

Autentizace k AP

- Open System authentication – k přihlášení stačí znát pouze SSID (*Service Set Identifier*), přenos dat je pak šifrován
- Shared-key authentication – nevýhoda je posílání řetězce v zašifrované a později i v nezašifrované formě [10]



Obrázek 2-3 Shared-key autentizace, WEP

Vylepšení nabízí WPA (*WiFi Protected Access*). Ta využívá také šifry RC4, jako v případě WEP, z důvodu zpětné kompatibility. Nově se zde pracuje s protokolem TKIP (*Temporal Key Integrity Protocol*), který zavádí dynamické klíče. Novinkou je možnost použití oboustranné autentizace.

TKIP mění dynamický klíč jednou za 10 000 paketů. Tímto opatřením je znemožněno odposlechnout dostatečné množství paketů k odhalení klíče. Přidává také lepší zabezpečení přenášených zpráv – MIC (*Message Integrity Check*), které zabraňuje útočníkovi pozměnit již vyslané pakety. K obraně proti takovým útokům slouží i číslování paketů. WPA dále zvětšuje vektor IV na velikost 48 bitů. Nevýhodou je snížení rychlosti v sítí o 5 až 15%.

Autentizace může být uskutečněna pomocí 802.1x nebo s použitím PSK (*Pre-shared Key*). PSK je sdílený klíč, pomocí kterého se uživatelé přihlašují k AP. Této metody využívají především nefiremní uživatelé. WPA bylo vytvořeno jako náhrada WEP před příchodem 802.11i (WPA2).

Standard 802.11i, jež nabízí ověřování pro firemní zákazníky, přináší WPA2 využívající protokol CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code*), šifrující provoz pomocí AES (*Advanced Encryption Standard*), místo dříve užívané RC4, který také zajišťuje zabezpečení rámců pomocí MIC a číslování rámců. K přihlašování je tedy možné využít jak PSK, tak i 802.1x.

802.1x se využívá k autentizaci uživatele, a to např. pomocí ověřovacího serveru RADIUS využívajícího protokol EAP (*Extensible Authentication Protocol*). EAP protokol zajišťuje přenos přihlašovacích informací od klienta k serveru RADIUS. Využívá se především ve firmách. Jeho výhodou je obousměrné ověřování jak klienta, tak i AP. [19]

2.1.6 802.11k (IEEE 2007) Radio Resource Management

Vylepšuje měření a informace o síti mezi AP a klienty. Např. měřením kanálu zjistí AP od klienta vysláním *probe* rámců úroveň signálu a zátěže, a tak bude moci vybrat vhodný kanál bez rušení.

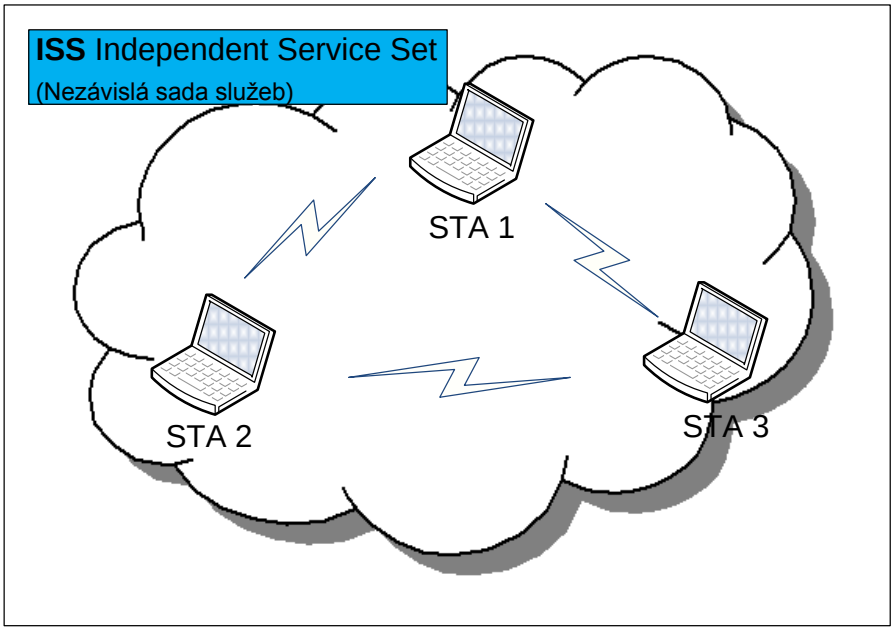
Probe rámce se využívají i pro aktivní skenování. Klient vyšle rámec *probe request* (zde jsou informace o SSID, podporovaných rychlostech a informace přidané výrobcem) a od AP dostane odpověď v podobě rámce *probe response* (který je podobný *beacon* rámci). [16]

2.2 Typy sítí

2.2.1 Ad-Hoc sítě

Ad-Hoc sítě jsou v podstatě jen spojením jednotlivých stanic bez přítomnosti AP. Stanice mezi sebou komunikují přímo dle potřeby. Tento způsob ale není vhodný pro dlouhodobější spojení či rozsáhlejší sítě.

Stanice se střídají ve vysílání *beacon* rámců, a tímto způsobem je dosaženo jejich vzájemné časové synchronizace. Vzájemná synchronizace je využita např. při režimu snížené spotřeby, kdy se stanice probouzí v určitý čas na příjem *beacon* nebo datového rámce, a tím šetří energii. Což je nutno hlavně u mobilních zařízení.

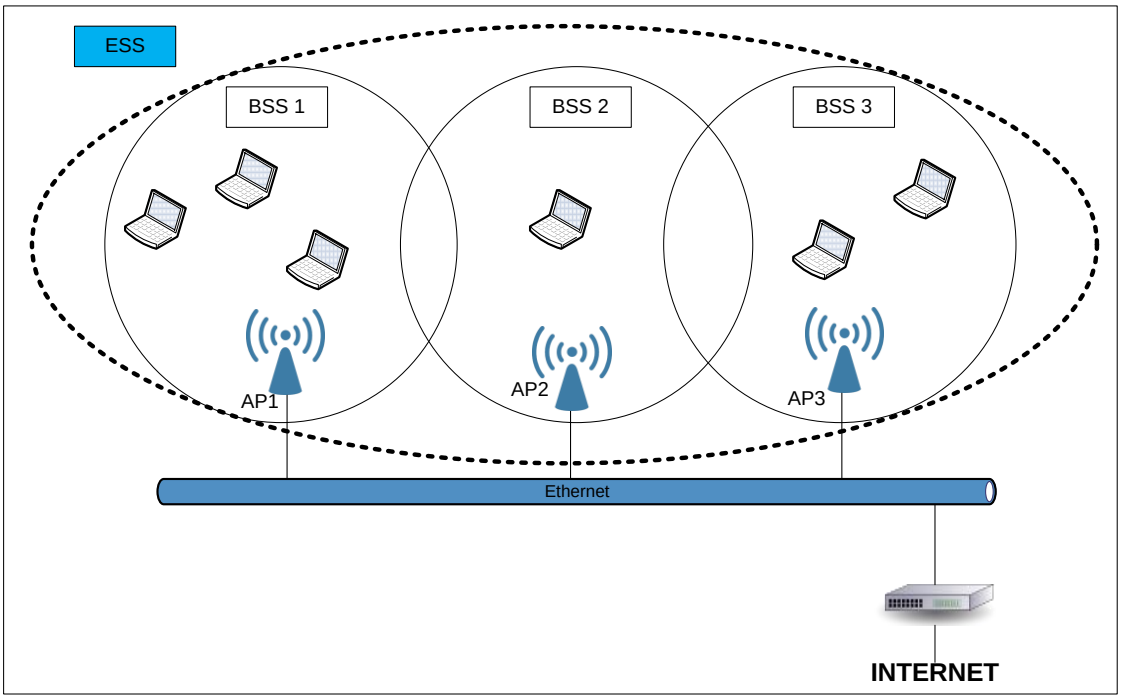


Obrázek 2-4 Schéma Ad-hoc sítě s 3 klienty

2.2.2 Infrastrukturní sítě

Jsou to rozsáhlejší sítě s jedním, nebo více přístupovými body. Jejich základním prvkem je tedy přístupový bod, který zde plní řadu funkcí (podpora a řízení QoS, NAT - *Network address translation*, DHCP - *Dynamic Host Configuration Protocol* apod). V tom nejjednodušším případě souží jako most mezi bezdrátovou a metalickou sítí. [10]

BSS (základní soubor služeb - Basic Service Set) - základní stavební blok sítě 802.11, v němž stanice komunikují pomocí AP.



Obrázek 2-5 Infrastrukturní síť

ESS (rozšířený soubor služeb – *Extended Service Set*) - více AP v jednotlivých BSS propojených přes metalické vedení. Stanice mezi sebou mohou v rámci ESS komunikovat a využívat služby ESS, i přestože nejsou ve stejných BSS.

Standard 802.11 umožňuje propojení více BSS dohromady, díky čemuž můžeme pokrýt větší oblast. Jednotlivé AP se propojí přes metalické vedení, a tím umožní, aby uživatel mohl volně přecházet z jedné BSS do druhé. Využívá k tomu službu zvanou roaming. Stanice se sama přepojí *reassociation* v závislosti na síle signálu, šířky pásma nebo ztrátovosti paketů. Podmínkou je, aby sítě měly nastaveno stejné SSID a z 20 až 30% se překrývaly.

Podpora služby roaming se řeší ve standardu 802.11f. Ten upřesňuje komunikaci mezi AP – např. protokol IAPP (*Inter-Access Point Protocol*) nebo MIP (*Mobile IP*).

IAPP – při přesunu klienta od jednoho AP k druhému při zachování stejné IP adresy.

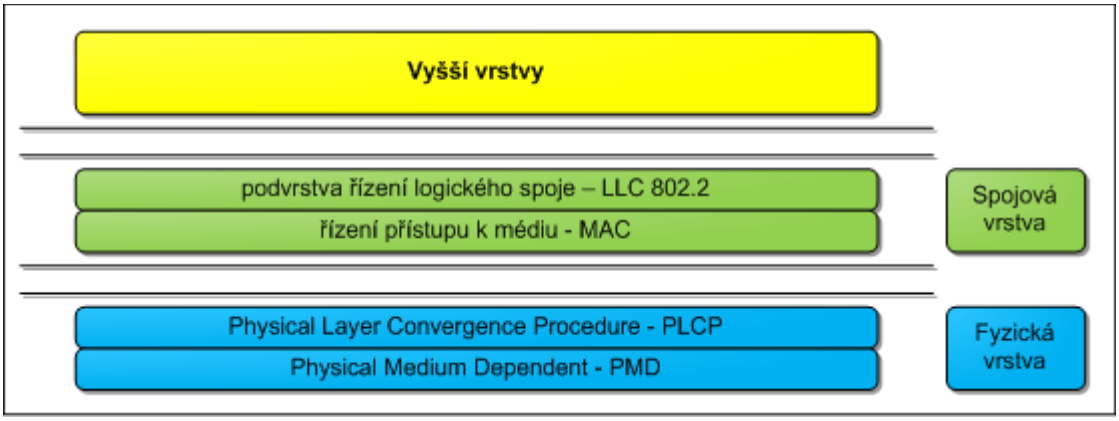
MIP – přesunuje-li se klient z jedné sítě do druhé pak AP (*Home Agent*) zapouzdří paket a pošle ho „tunelem“ k novému AP (*Foreign agent*), ke kterému se stanice nově připojí. Ten z paketu oddělí přidanou IP hlavičku a pošle ho přímo ke klientovi. [10]

Služby v sítí:

- Autentizace/Deautentizace (*Authentication/ Deauthentication*)
  - stanice se prokazuje u AP a naopak
- Asociace / Deasociace (*Association/ Disassociation*)
  - vlastní přiřazení stanice k jednomu AP a naopak; stanice pak může využívat služby v síti
- Reassociation
  - u roamingu stanice se přehlásí od jednoho AP ke druhému (přechod mezi BSS v rámci jedné ESS)
- Distribuce (*Distribution*)
  - přenos rámců mezi AP v ESS
- Utajení dat (*Data confidentiality*)
  - šifrování dat při přenášení
- MSDU doručování (*MAC Service Data Unit delivery*)
  - doručování a posílání paketů
- Higher layer timer synchronization – QoS
  - umožňuje použít více aplikací v jednom čase (proudové vysílání zvuku nebo videa)
- QoS plánování provozu (*QoS traffic scheduling*)
  - fronty; značení paketů pro služby QoS [1]

3 802.11

Standard 802.11 upravuje dvě vrstvy modelu ISO OSI, a to vrstvu linkovou (spojovou) a fyzickou. Což je výhoda především vzhledem k zachování stejných protokolů na vyšších vrstvách. Z tohoto důvodu se může využívat nezměněný protokol vyšších vrstev, jako je např. HTTP apod.



Obrázek 3-1 Vrstvy v 802.11 [16]

Maximální délka rámce u 802.11 je 2 346 B.

Frame Control	Duration /ID	ADDR1	ADDR2	ADDR3	Sequence Control	ADDR4	Data	FCS CRC
2B	2B	6B	6B	6B	2B	6B	0 -2,312B	4B

Obrázek 3-2 Obecný tvar rámce [23]

Protocol Version	Type	Subtype	To DS	From DS	More Flag	Retry	Pwr Mgt.	More Data	Protected Frame	Order
2b	2b	4b	1b	1b	1b	1b	1b	1b	1b	1b

Obrázek 3-3 Frame control rámec [23]

Ukázka datového rámce z programu Wireshark - viz PŘÍLOHA 1.

Popis jednotlivých částí datového MAC rámce:

- Frame control – informace týkající se přenášeno rámce
  - Protokol version – určuje verzi protokolu
  - Type – typ rámce; v závislosti na něm se mění i délka rámce
    - Ovládací (*Control*) – hodnota 01
    - Řídící (*Management*) – hodnota 00
    - Datový – hodnota 10
  - Subtype – označuje podtyp rámce – např. ovládací - RTS, CTS, ACK (např. RTS rámec má Type 00 a Subtype 1011)
  - Flags
    - To DS – pokud jsou data přenášena do distribučního systému, je hodnota 1
    - From DS – jsou-li data přenášena z distribučního systému je hodnota 1
    - More fragments – za rámcem následují další rámce – hodnota 1
    - Retry – hodnota 1 značí opětný přenos předchozího rámce
    - Power Management – udává, v jakém režimu bude stanice po úspěšné výměně rámců; hodnota 1 značí, že stanice bude v režimu snížené spotřeby, hodnota 0 znamená aktivní režim stanice; rámce vyslané od AP mají vždy hodnotu 0
    - More data – hodnota 1 oznamuje, že ve vyrovnávací paměti jsou uložena data pro stanici; hodnota 1 se používá i při vysílání dat typu broadcast/multicast, kdy AP má ještě co vysílat
    - Protected Frame – udává typ zabezpečení (WEP, WPA, WPA2)
    - Other – hodnota 1 je pro pakety služby *Strictly Ordered*, které už nejsou dále zpracovávány, 0 je pro QoS
- Duration – určuje dobu trvání přenosu, a tím i alokaci média (výpočet intervalu NAV - *Network Allocation Vector*)
- ADDR1 – ADDR4 – adresa zdroje, cíle, přenašeče a přijímače v závislosti na hodnotách ve *Frame control*
- Sequence kontrol – využívá se pro kontrolu přijatých rámců, a tak lze vyřadit duplicitní rámce
- FCS (CRC) – kontrolní součet; používá se k detekci chyb během přenosu či ukládání dat [2] [23]

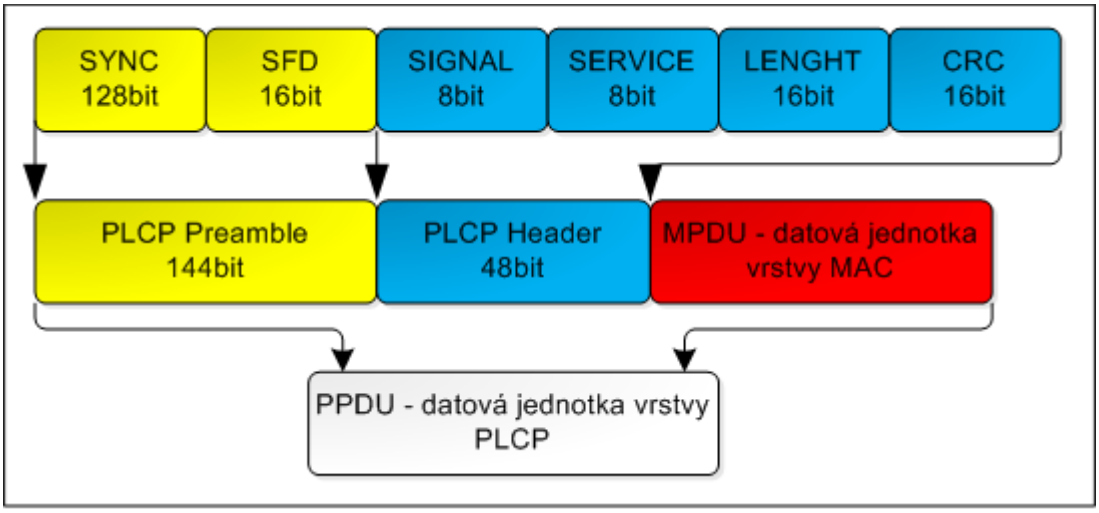
3.1 Fyzická vrstva

Tato vrstva upravuje fyzikální parametry a určuje, jakým způsobem se budou data vysílat. Obsahuje následující podvrstvy:

PMD (*Physical Medium Dependent*) – přenosové rozhraní, které nabízí funkce související s rádiovým přenosem – kmitočet, typ klíčování atd. [23]

PLCP (*Physical Layer Convergence Procedure*) – tato podvrstva přidává svou hlavičku k přenášeným rámcům a v ní se určuje např. druh modulace. Tím zajišťuje, že rámec je nezávislý na modulaci - mění se jen hlavička PLCP. V rámci této podvrstvy je poskytována služba CCA (*Clear Channel Assessment*).

CCA pomáhá vrstvě MAC ke zjištění, zda médium, na kterém se bude vysílat, je volné. CCA na fyzické vrstvě porovná signál na anténě. Podle úrovně signálu určí, zda je médium volné nebo obsazené. [17] [23]



Obrázek 3-4 Rámec s hlavičkou PLCP při použití DSSS [23]

PLCP hlavička je vždy přenášena rychlostí 1 Mbit/s za použití modulace BPSK (*Binary Phase Shift Keying*) tak, aby ji každý z klientů mohl přijmout nezávisle na používané normě (802.11b, g, n). Zajišťuje se tím také nižší chybovost při předávání důležitých údajů k přenosu, ale za cenu značné režie.

(Pozn. BPSK je binární fázové klíčování – změn z 0 na 1 je signalizována změnou fáze nosného signálu o 180^{o}.)

Popis hlavičky PLCP (viz obrázek 3-4):

- SYNC – slouží k synchronizaci; hodnotou jsou samé 1 (jejich počet závisí na tom, zda jde o dlouhou nebo krátkou hlavičku)
- SFD – určuje začátek PLCP hlavičky; binární hodnota je 1111001110100000
- SIGNAL – určuje typ modulace a rychlosti, např. u DSSS
    - '0Ah'(bin 00001010) pro 1 Mbit/s DBPSK (*Differential Binary Phase Shift Keying*)
    - '14h'(bin 00010100) pro 2 Mbit/s DQPSK (*Differential Quadrature Phase-Shift Keying*)
- SERVICE – je zde např. bit pro indikaci stejného hodinového signálu pro vysílání a bitovou synchronizaci; tyto bity slouží také pro výpočet délky datové jednotky
- LENGHT – délka přenosu MPDU v μs
- CRC – cyklický redundantní počet, zabezpečuje SIGNAL, SERVICE, LENGHT

PLCP preamble může mít 2 tvary:

- dlouhý PLCP preamble - 128 + 16 bitů; musí ho podporovat všechny zařízení
- krátký preamble - 56 + 16 bitů; využívá se u VoIP (zmenšení zpoždění); volitelná podpora [1] [10]

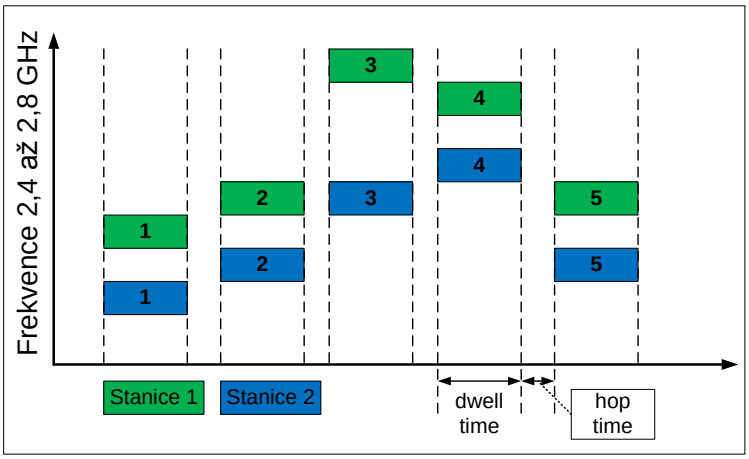
3.1.1 Typy přenosů

3.1.1.1 FHSS (F*requency hopping spread spectrum*)

Přenosová technika byla původně určena pro vojenské využití. Funguje na základě frekvenčního multiplexu. Vysílač vysílá data po předem určitý čas na známé frekvenci (*dwell time* 200 – 400 ms), a poté přeskočí (*hop time* 30 ms) na další frekvenci. Tento postup se stále opakuje a je „náhodný“. Údaje jako je délka vysílání a počet přeskoků na určité frekvenci si spolu stanice musí vyměnit - synchronizovat je. V případě selhání synchronizace by totiž stanice nebyly schopny navázat spojení nebo uskutečnit přenos dat.

Velkou výhodou je větší odolnost vůči rušení a kolizím. Frekvence se neustále mění, nastane-li kolize, opakující se paket je vyslán na jiné frekvenci. Další výhodou je pak možnost použití většího počtu vysílačů v pásmu 2,4 GHz, každý pak pracuje na jiné frekvenci.

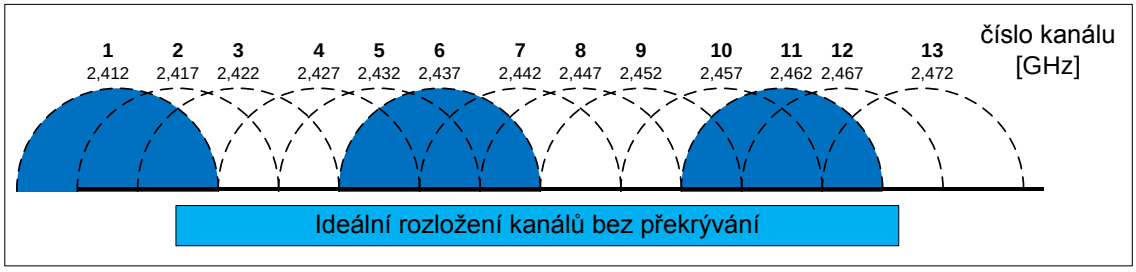
Dostupná frekvenční šířka 83,5 MHz je rozdělena do 79 kanálů o šířce 1 MHz. Zbylé 4,5 MHz slouží jako ochrana proti interferencím ze sousedních kanálů. Přenosovou techniku FHSS využívá např. technologie Bluetooth. [10] [16] [23]



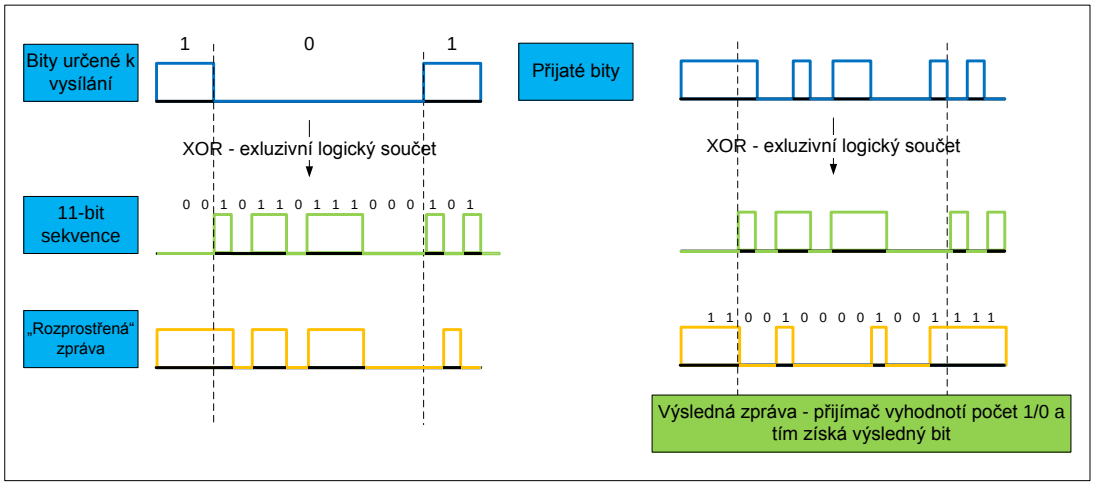
Obrázek 3-5 FHSS

3.1.1.2 DSSS (*Direct Sequence Spread Spectrum*)

U této metody přenosu se využívá šířka pásma 22 MHz. Každý bit vysílaný vysílačem se vynásobí posloupností bitů, a tím se zvětší jeho šířka pásma. DSSS využívá v ČR 13 kanálů (2,412 – 2,472 GHz). Pro jeden kanál je potřebná šířka 22 MHz, plus ochranné pásmo 5 MHz. Z toho vyplývá, že nemůžeme využít všech 13 kanálů, aniž by se nepřekrývaly, a tedy i navzájem nerušily. Maximální počet dostupných kanálů bez překrývání je roven číslu 3. Např. kanály 1, 6, 11. Důvodem k využití širšího pásma je možnost snížení vysílacího výkonu, čímž dojde ke zmenšení možného rušení okolních systémů. Přenášené bity jsou také odolnější vůči úzkopásmovému rušení. Pro jejich větší odolnost se jeden bit kóduje 8 nebo 11 bity (1 chip), které jsou následně vyslány. Princip metody je naznačen na Obrázku 3-7. [23]



Obrázek 3-6 DSSS rozložení kanálů



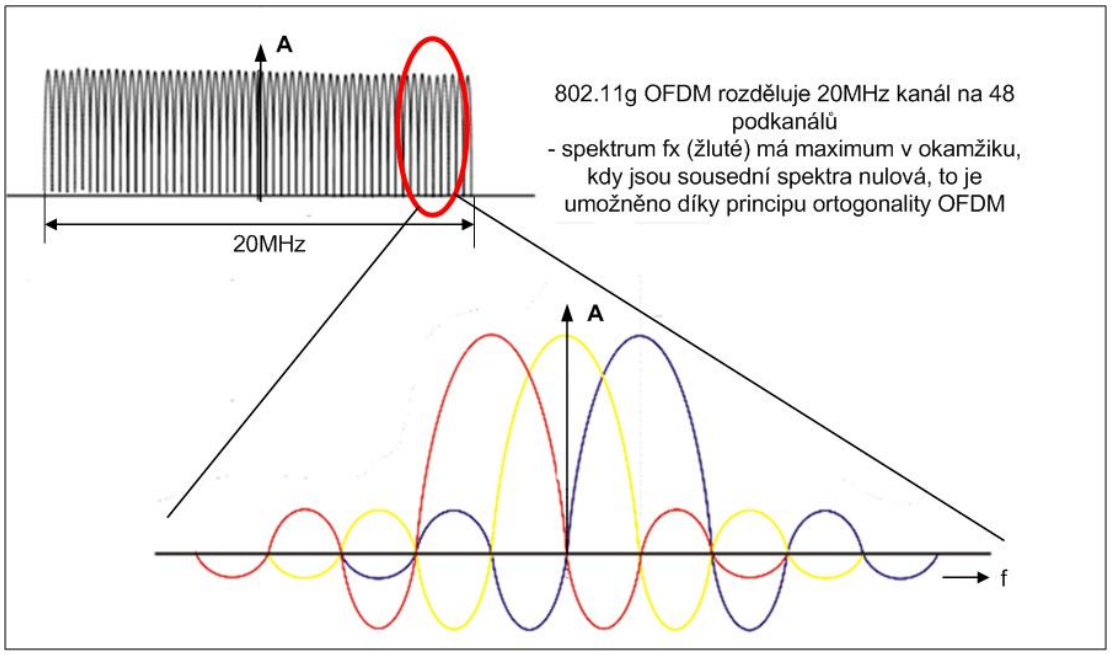
Obrázek 3-7 DSSS příjem a vysílání sekvence bitů u 802.11b 5,5; 11 Mbit/s [10]

3.1.1.3 OFDM (*Orthogonal Frequency Division Multiplex*)

Přenosová technika OFDM je založena na rozkladu signálu do více paralelních toků, které mají nižší rychlost. To je výhodné z hlediska chybovosti. Pomalejší paket je méně náchylný na chybovost, než ten rychlejší. Mezi intervaly symbolů je také vkládán tzv. ochranný interval (*guard interval*) o hodnotě např. 800 ms u 802.11a (u 802.11n je zkrácen na 400 ms).

Každý signál má svou nosnou frekvenci a každý zvlášť je modulován digitální modulací, např. QAM (*Quadrature amplitude modulation*). OFDM podporuje rychlosti 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s. Nižší rychlosti jsou modulovány DBPSK a DQPSK, u vyšších rychlostí je použito 16 nebo 64 QAM. Výsledná rychlost je pak dána součtem paralelních spojení. Výhodou je vysoká rychlost a dobrá odolnost vůči vícecestným interferencím. Důvod je ten, že bity se přenáší pomaleji, a tak se jeho zpoždění, přijímané z jiné cesty, tolik neprojeví.

Další výhodou je efektivnější využití frekvenčního pásma, protože subkanály se překrývají (Obrázek 3-8). Používá se např. v 802.11a, g, n (802.11n využívá i jiné technologie např. MIMO). [10] [14] [17] [23]



Obrázek 3-8 OFDM (802.11g) [6]

(Pozn. Důvod k využití vícestavové modulace QAM je následující - šetří šířku pásma a umožňují tak dosáhnout vyšších rychlostí. Na druhé straně existuje nevýhoda - při rušení je obtížné identifikovat od sebe jednotlivé stavy.)

3.2 Spojová vrstva

Podvrstva MAC řídí přístup stanice k médiu. To je důležité, protože v jednom okamžiku smí vysílat pouze jedna stanice. Aby situace, kdy začne vysílat více stanic najednou, nenastala, používají se dvě koordinační funkce - distribuovaná DCF a centralizovaná PCF.

3.2.1 DCF (*Distributed Coordination Function*)

Jako základ pro tuto metodu slouží CSMA/CA (*Carrier Sense Multiple Access with Collision Detection*), což je mechanismus předcházející kolizím. Distribuovaná koordinační funkce (dále jen DCF) poskytuje jen službu typu *best effort*. To znamená, že nepodporuje žádné řízení front nebo provozu. Používá dvě techniky – odložení vysílání (*back off*) a mezirámcové mezery (*IFS – InterFrame Space*). Pracuje s tzv. oknem soutěžení (*contention window - CW*), jehož velikost určuje interval $<CW_{min}, CW_{max}>$. Jsou to hodnoty, kterých může velikost okna dosáhnout. Hodnoty CW jsou násobky *slot time* (20µs pro 802.11b). Řešení v podobě násobků *slot time* je výhodné. V případě kolize zaručuje zvolení stejného čísla u jednotlivých stanic.

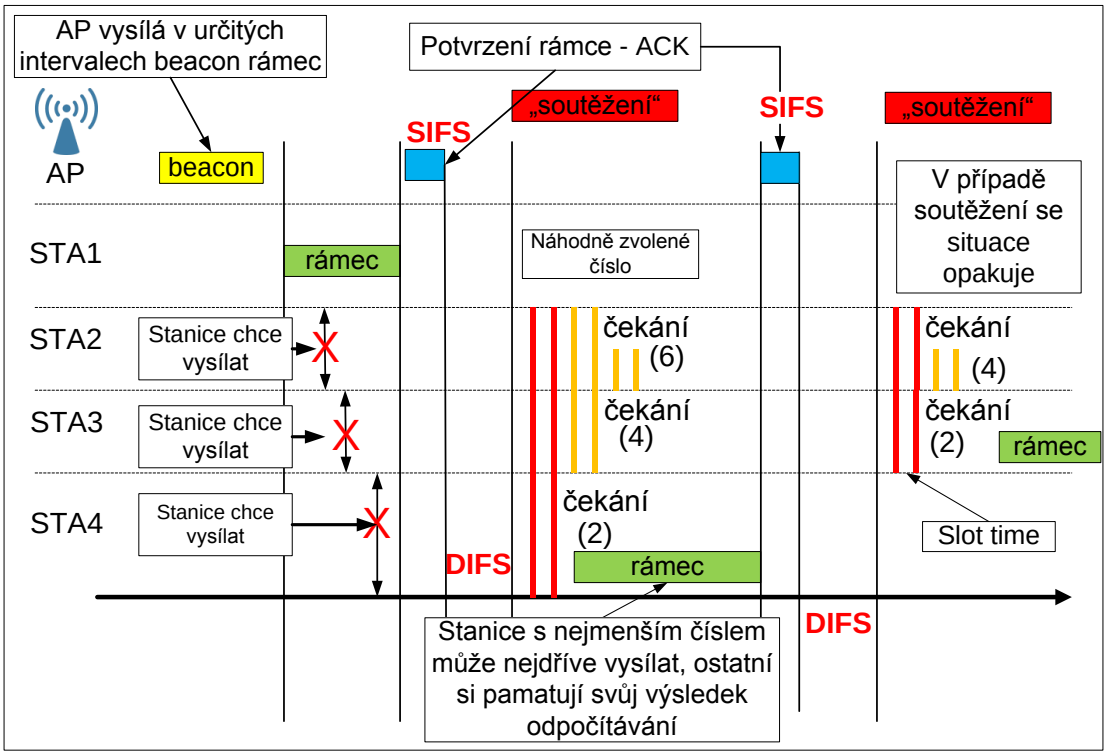
Stanice, která chce vyslat rámec, nejdříve naslouchá, zda je médium volné. Pokud tomu tak je, stanice počká dobu mezirámcové mezery DIFS (*DCF InterFrame Space* – 50 µs pro 802.11b). Je-li médium i poté stále volné, vygeneruje náhodné číslo v intervalu 0 až CW. Počáteční hodnota CW je dána parametrem CW_{min}. Po získání náhodného čísla stanice zahájí odpočítávání, a přitom stále kontroluje obsazenost média. V případě dokončení odpočítávání, což je možné pouze, je-li médium stále volné, začne stanice vysílat. Dokončí-li některá ze stanic odpočet dříve, ostatní stanice si zapamatují zbývající délku čekacího intervalu. Toto číslo je pak použito v dalším soutěžení o přístup k médiu.

Pokud si dvě stanice zvolí stejné číslo, dochází ke kolizi. Přeruší se vysílání a následně proběhne odklad vysílání (*back off*). Poté je znovu zvoleno náhodné číslo z intervalu CW, který se po každé kolizi zvětšuje podle vzorce:

$$CW_{nové} = (CW_{stará} + 1) \times PF - 1$$

A to až do hodnoty CW_{max}. PF (*Persistence Factor*) je koeficient zvětšení. U metody DCF je roven dvěma, a tak se CW při každé kolizi zdvojnásobí. [11]

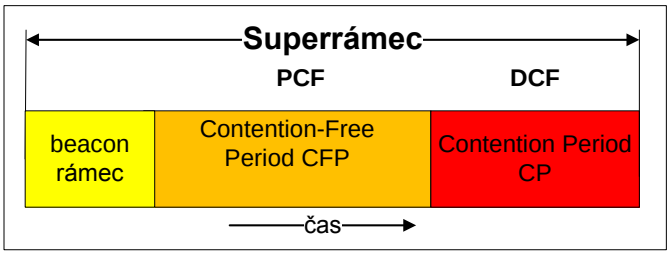
Po úspěšném přenosu se velikost CW vrací do své původní hodnoty. Přijímač počká dobu SIFS (*Short IFS* – 10 µs pro 802.11b). Tato doba je kratší než DIFS a slouží k odeslání ACK - potvrzení přijetí paketu (nebo RTS, CTS). Potvrzování je nutné z důvodu ztráty paketu cestou k přijímači např. při nekvalitnímu signálu. Stanice by poté nemohla rozpoznat, zda byl paket doručen a zda má vysílat dál, nebo vysílání předchozího rámce opakovat. *(Pozn. velikost CW pro 802.11b se pohybuje od 31 do 1023.)* [12] [14][16][18][19]



Obrázek 3-9 DCF - soutěžení a potvrzování rámců

3.2.2 PCF (*Point Coordination Function*)

Tato funkce je doplňková, pokud má fungovat musí ji podporovat všechna zařízení v sítí. Dnes se tato metoda již nevyužívá. V případě jejího použití lze časový interval mezi rámci *beacon* rozdělit na dva časové úseky bez a se soutěžením. Intervaly CFP - (*Contention Free Period)* a CF - (*Contention Period*) souhrnně označované jako superrámec.

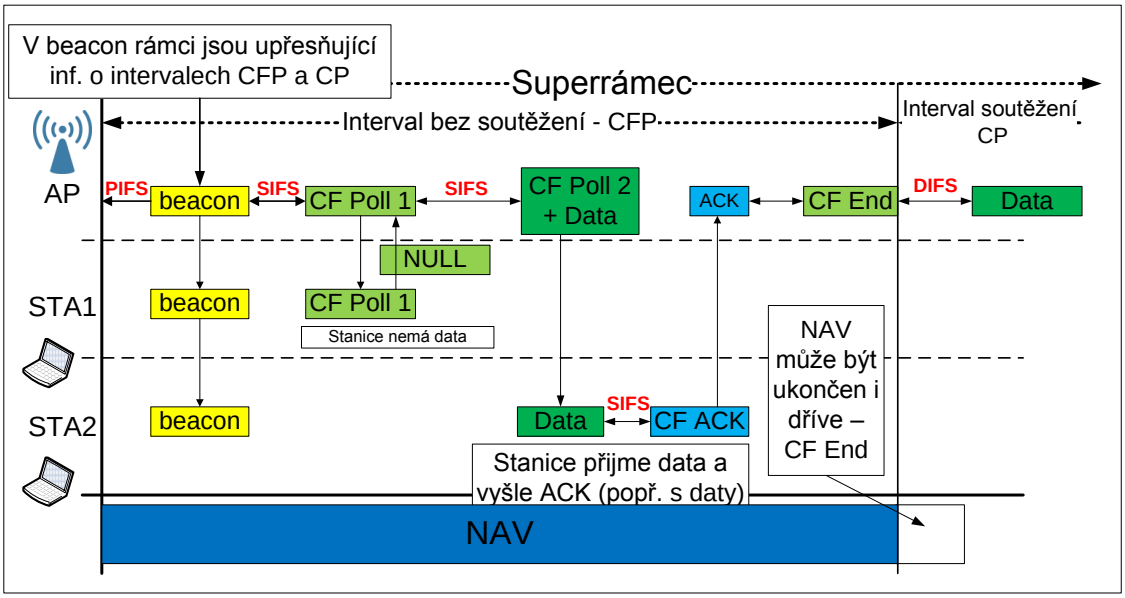


Obrázek 3-10 Superrámec

Stanice podporující PCF se zaregistrují u AP, který si vytvoří jejich seznam. AP po zjištění volného média počká dobu PIFS (30 µs pro 802.11b; PIFS < DIFS), a pak vyšle *beacon* rámec. *Beacon* rámec je v tomto případě důležitý, protože určuje dobu trvání CFP intervalu v parametru - *CF parameter setting*. Po vyslání *beacon* rámce počká AP dobu SIFS (10 µs pro 802.11b), a poté začne interval bez soutěžení – CFP. V tomto intervalu AP postupně rozesílá stanicím dotazy CF-Poll, zda pro něj mají data a popřípadě přiděluje prostor k vysílání. V případě, že stanice data má, odpoví potvrzujícím rámcem CF-ACK a začne je odesílat. Stanice a AP pro urychlení komunikace mohou a nemusí posílat rámce CF spojené s daty – CF-Poll + Data, nebo i s potvrzením – Data + CF-ACK. Nemá-li stanice data, pošle AP prázdný rámec (NULL), který vyzve dotazem další stanici na seznamu. AP se postupně dotazuje dalších stanic do doby konce CFP intervalu, nebo než zašle CF-End rámec. Pak začíná interval soutěžení – CP.

Nevýhodou PCF je nerozlišování priorit a možnost, že dlouhý rámec jedné stanice může zablokovat přenos ostatních stanic. Interval vysílání *beacon* rámců není totiž v tomto případě pevně stanoven a může se v závislosti na délce rámců měnit. S ním se mění i doba trvání celého superrámce. Ve standardech je pouze upřesněna maximální délka intervalu CFP, a to na dobu přenosu dvou rámců o maximální velikosti (2346 B), včetně rámců *beacon*, CF-Poll a mezirámcových mezer. Dalším omezením je přenos minimálně jednoho rámce o maximální velikosti včetně rámců a mezer v intervalu CP.

V následujícím intervalu soutěžení je využita funkce DCF i s její nevýhodou. Rámce v tomto intervalu soutěží o možnost přístupu k médiu, a tak nelze zajistit jeho přesný konec, a tím pádem ani přesné vyslání následujícího *beacon* rámce. Detailnější princip PCF je znázorněn na Obrázku 3-11. [16] [18] [23]



Obrázek 3-11 CFP a CP interval

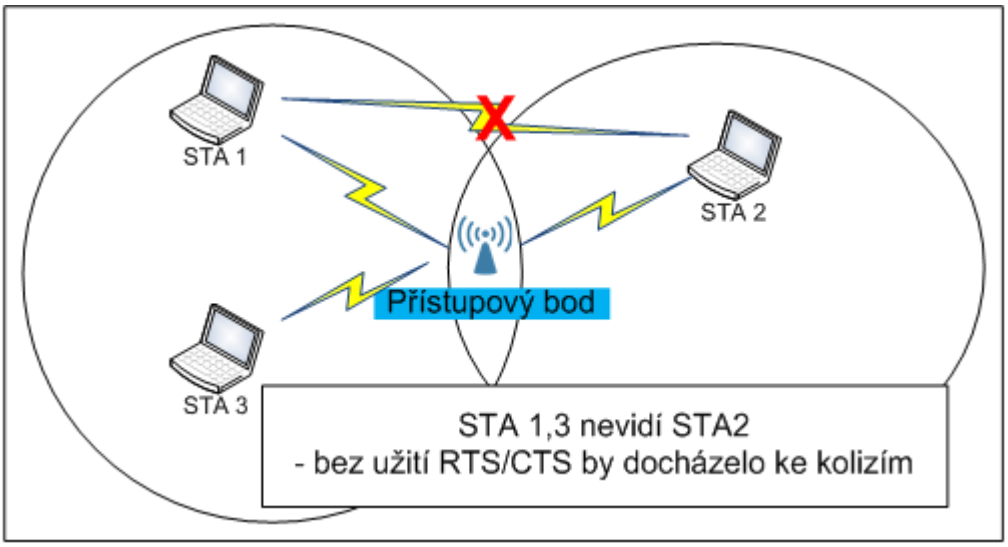
Beacon rámec patří mezi řídící rámce a jsou v něm přenášeny v určitých intervalech informace týkající se např. podporovaných rychlostí, typu modulace, délky hlavičky na fyzické vrstvě a dalších přídavných služeb, které nabízí BSS či ESS. Ukázka *beacon* rámce zachycená programem Wireshark – PŘÍLOHA č. 1

Popis některých informací v *beacon* rámci:

- Timestamp (8B) – stanice jej využívá k synchronizaci s AP
- Beacon Interval (2B) – interval odesílání *beacon* rámců; využívá se při probouzení stanic z režimu spánku (snížené spotřeby)
- Capability Information (2B) – informace např. o zabezpečení (WEP), použité modulaci, podpoře QoS, délce slot time atd.
- SSID parameter set (6B) – informace o názvu sítě (SSID – 32 ASCII znakový řetězec identifikující bezdrátovou síť)
- BSSID – MAC adresa přístupového bodu
- DS parameter set (3-7B) – informace o DSSS (např. číslo kanálu)
- Traffic Indication Map (TIM) – v tomto poli jsou umístěny MAC adresy stanic, pro které má AP data, a které jsou v režimu se sníženou spotřebou (PSP - *Power Save Polling*). Stanice se probouzí na příchod *beacon* rámce, pokud najde svoji MAC adresu v poli TIM, zůstane aktivní a přijme data. V opačném případě se vrátí do režimu spánku. [2] [4]

3.2.3 Skrytý uzel

Tento problém se týká hlavně sítí provozovaných ve venkovním prostředí na větší vzdálenosti. Využití WiFi sítí bylo původně plánováno především do budov, ve kterých byla vysoká pravděpodobnost blízké vzdálenosti jednotlivých stanic. Stanice byly ve vzájemném dosahu, a tak měly možnost detekovat obsazení média některou z ostatních stanic. Ovšem při zvětšování jejich rozestupu na pokrytí větší vzdálenosti, nebo s využitím směrových antén, začne stoupat počet kolizí. Stanice nebudou schopny detekovat obsazené médium, začnou tak odesílat data v době vysílání jiné stanice.

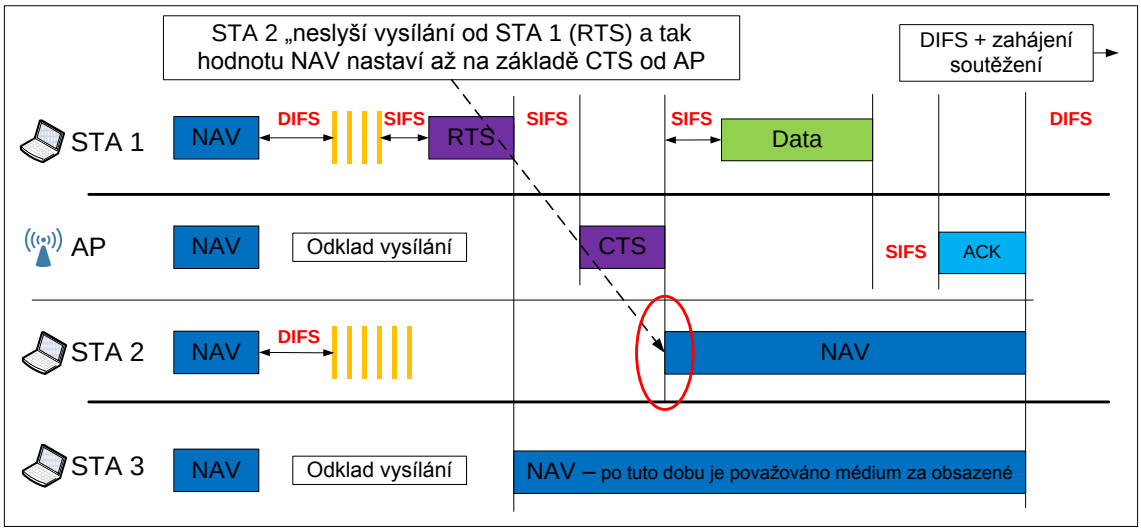


Obrázek 3-12 Problém skrytého uzlu

Metoda RTS/CTS využívá tyto rámce:

- RTS (*Request To Send*) – požadavek na přidělení prostoru k vysílání
- CTS (*Clear To Send*) – odpověď na rámec RTS

RTS/CTS funguje na principu žádosti a potvrzování. Stanice chce vyslat data. Zjistí stav přenosového média. Je-li volné, stanice vyšle RTS rámec, a tím oznámí AP potřebu vyslat data. AP, pokud je volný, odešle rámec CTS. Stanice pak ví, že může zahájit vysílání. Po odeslání dat počká na potvrzení rámcem ACK. Pro snížení možnosti kolizí se v rámcích RTS a CTS posílají i doby trvání přenosu. Ostatní stanice, i když vysílací stanici „nevidí“, nastaví si identifikátor vektoru NAV (*Network Allocation Vector*) na dobu trvání přenosu. V tomto čase budou stanice považovat médium za obsazené. Čímž se riziko kolizí zmenšuje jen na dobu vysílání rámce RTS. Rámec CTS vyslaný AP zachytí už všechny stanice, protože AP musí být v dosahu všech stanic.



Obrázek 3-13 Metoda DCF v kombinaci s RTS/CTS [6]

Nevýhoda této metody je neefektivní využití sítě zablokováním média po dobu vysílání jedné stanice. Pokud jsou přenášeny malé pakety, propustnost se ještě zmenší. Využití RTS/CTS sníží propustnost v síti zhruba o 20%. [10][15]

Ovládací rámce – CTS/RTS

FC	Doba trvání	Receiving Station Address – RA	FCS (CRC)
2B	2B	6B	4B

Clear To Send (CTS), ACK

FC	Doba trvání	Receiving Station Address – RA	Transmitting Station Address – TA	FCS (CRC)
2B	2B	6B	6B	4B

Request To Send (RTS)

Obrázek 3-14 Rámce CTS/RTS

Pozn.: TA - MAC adresa vysílající stanice

RA je MAC adresa přejímací stanice

4 802.11e

Sítě WiFi nejsou na využívání služeb citlivých na zpoždění stavěny. V původním návrhu s využitím přístupové funkce DCF byl provoz řízen spravedlivě, ale nebyla zde žádná metoda na upřednostňování různých druhů provozu. Proto při větším zatížení rostly parametry ovlivňující provoz multimediálních služeb, jako je např. zpoždění, ztrátovost apod. Nedostatek v tomto návrhu má řešit nově vytvořený standard 802.11e., jehož úkolem je co nejlépe vyhovět moderním požadavkům na řízení kvality služeb. Musí zajistit co nejmenší hodnoty zpoždění, kolísání zpoždění, ztrátovosti a garantovat určitou šířku pásma pro jednotlivé druhy provozu. Ještě před odsouhlasením standardu 802.11e se objevila technologie WMM (*WiFi Multimedia*), jenž podporuje část funkcí z 802.11e. [2] [7]

Standard 802.11e rozšiřuje původní metody přístupu k bezdrátovému médiu DCF a PCF. Nově tak zavádí dvě koordinační funkce – EDCA (*Enhanced Distributed Coordination Function*) a hybridní HCF (*Hybrid Coordination Function*), které využívají dvě metody přístupu k médiu:

- EDCA (*Enhanced Distributed Channel Access*) – je využita při intervalu soutěžení (CP)
- HCCA (*HCF Controlled Channel Access*) – tuto metodu je možno použít jak v intervalu soutěžení, tak i bez něj (CP, CFP)

802.11e přidává novou sadu služeb – QBSS (*QoS supporting BSS*). Klienti s podporou QoS se nazývají QSTA a AP s podporou 802.11e Hybrid Coordinator – HC.

Dále přidává i několik neméně důležitých funkcí:

- APSD (*Automatic Power Save Delivery*) – lepší řízení spotřeby než PSP; stanice se samy rozhodují, kdy přejdou do aktivního režimu
- BA (*Block Acknowledgements*) – pro snížení režie se mohou potvrzovat celé bloky rámců
- NoACK – stanice nemusí potvrzovat přijaté rámce; zrychluje se tak provoz, čímž se snižuje zpoždění, ovšem za cenu zvýšeného rizika chybovosti
- DLS (*Direct Link Setup*) – zrychlení komunikace mezi HC a stanicemi pracujícími v úsporném režimu [2] [6] [11]

Pokud je v standard 802.11e podporován, je přidáno dvou bajtové pole *QoS Control* do MAC rámce. Hodnoty v něm se mění v závislosti na typu použitého rámce.

Příslušné rámce	bity 0 – 3	bit 4	bity 5 – 6	bit 7	bity 8 – 15
QoS CF-Poll rámce vyslané HC (AP s podporou QoS)	TID	EOSP	ACK pravidla	Rezervováno	Velikost TXOP (násobky 32μs)
Rámce QoS Data, QoS NULL, QoS Data +CF-ACK vyslané HC	TID	EOSP	ACK pravidla	Rezervováno	Stav vyrovnávací paměti HC
Rámec QoS Data vyslaný od QSTA	TID	0	ACK pravidla	Rezervováno	Požadovaná velikost trvání TXOP
	TID	1	ACK pravidla	Rezervováno	Velikost fronty (násobky 256B)

Tabulka 4-1 Pole QoS Control [1]

TID *(traffic identifier)* – identifikátor provozu; označuje typ dat z vyšších vrstev; buď pomocí pevně definovaných přístupových tříd (*Access Category*), nebo dynamicky přidělovaných (TSPEC - *Traffic Specification*) od vyšších vrstev (aplikací)

EOSP (*End Of Service Pole*) – určují, zda bude vysílání rámců ještě pokračovat nebo je rámec poslední

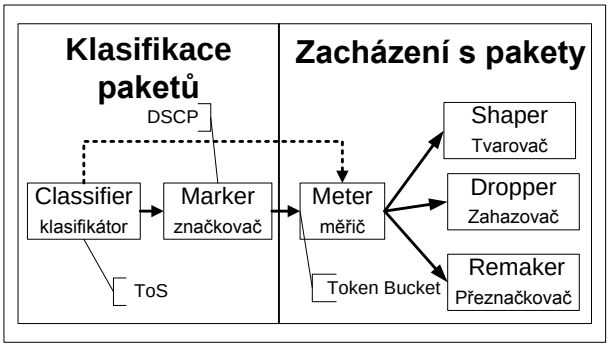
ACK pravidla – určuje, zda bude rámec potvrzen rámcem ACK (např. při vysílání typu broadcast/multicast je hodnota 01 a rámec potvrzení ACK není požadován).

V bitech 8 až 15 je určena maximální velikost intervalu TXOP (jeho hodnota je určena násobkem čísla 32 a jeho velikost je od 32 do 8160 μs a liší se v závislosti na přístupové třídě). Tento interval je vlastní povolení k vysílání, ale jen po předem určený čas, který je nastaven v závislosti na přístupové třídě. Dále se v těchto bitech nachází hodnota velikosti fronty, udávající počet rámců stejné priority čekajících ve frontě. V neposlední řadě také požadovaná velikost trvání TXOP (TXOP *Duration Requested Field*), kde QSTA při módu HCCA nastavuje požadovanou dobu potřebnou k přenosu svých dat. Při EDCA se tato hodnota ukládá do pole *QoS Info* v *EDCA Parameter Set* element. [1]

4.1 WMM (*Wireless Multimedia*)

4.1.1 Technologie Diferencovaných služeb (DiffServ)

Standard WMM je založen na architektuře *diffServ*, která pracuje na principu zacházení s pakety na základě jejich klasifikace (obrázek 4-1).



Obrázek 4-1 Architektura DiffServ [10]

- **Klasifikátor (classifier)**

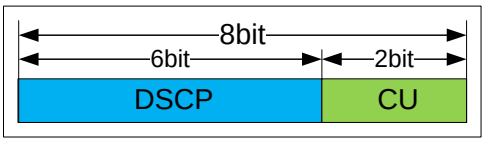
Příchozí pakety jsou identifikovány, a poté roztříděny podle jednoho nebo více kritérií do několika tříd. Jedno z kritérií může být např. zdrojová/cílová adresa nebo port.

- **Značkovač (marker)**

  Paketům je přidělena značka, podle které s nimi směrovače zacházejí. Jsou specifikovány 3 základní kategorie chování v rámci skoku mezi směrovači - PHB (*Per Hop Behavior*).

  - Expedited Forwarding (EF) – absolutní garance hodnoty zpoždění apod.; neefektivní využití sítě; složité, srovnatelné s např. virtuálním okruhem
  - Assured Forwarding (AF) – menší priorita než EF; čtyři skupiny podle možnosti přidělení prostředků směrovače (např. velikost vyrovnávací paměti apod.), a každé z nich je možno přidělit jednu ze tří priorit k zahození paketu
  - Best Effort (BE) – není využíváno žádných priorit, základní provoz

Tyto značky jsou uloženy do osmi bitového pole pojmenovaného ToS (*Type of Servic).* Rozlišují provoz do 64 tříd, nazývají se DSCP (*Differential service code point*) a využívají šestici bitů. Zbylé dva jsou pro budoucí využití.



Obrázek 4-2 Pole DS (*differentiated services*)

- **Měřič (meter)**

  Měří každý datový tok. V případě, že tento tok splňuje určité podmínky, např. datový objem nebo nedochází k přeplnění fronty, je přeposlán na výstup. Není-li tomu tak, je třeba ho upravit – zahozením, přeznačkováním nebo pozdržením ve vyrovnávací paměti. K měření se používá technika zvaná „*token bucket*“. Tuto techniku lze přirovnat k nádobě kuliček, které jsou postupně přidávány konstantní rychlostí nebo odebírány na výstupu. Jedna kulička odpovídá jednomu bajtu. Pokud paket nedostane počet kuličku odpovídající jeho velikosti, je zahozen.

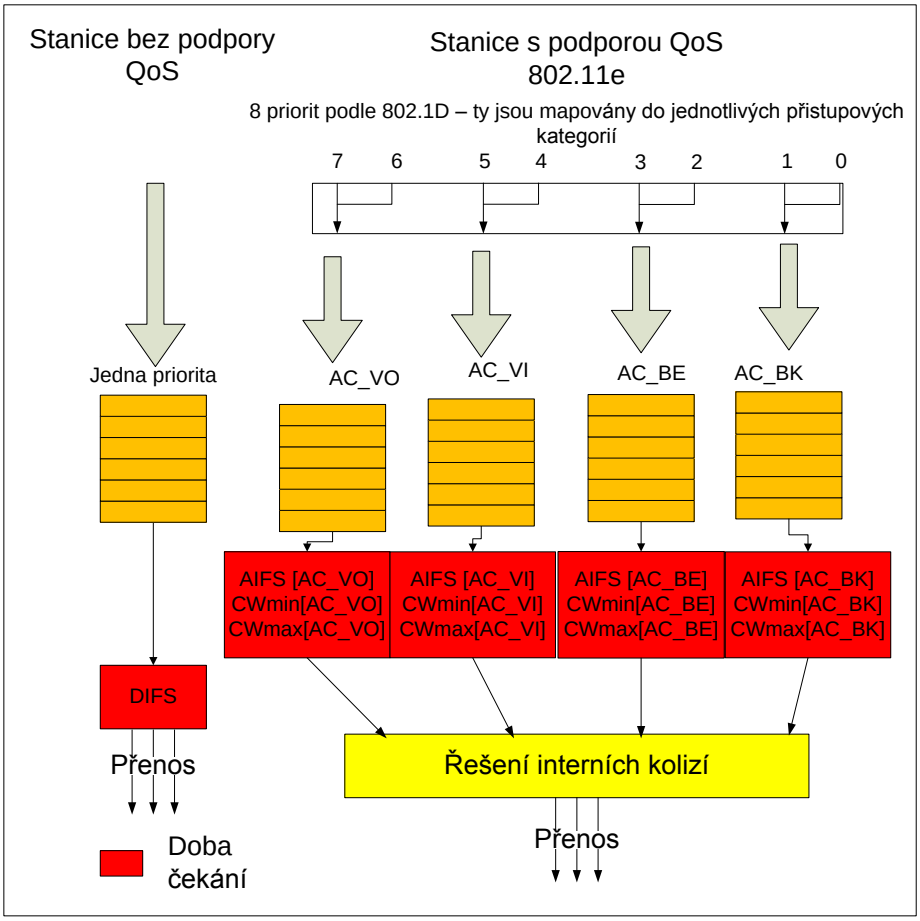
4.1.2 Popis WMM

Metoda WMM (dříve WME - *Wireless Media Extension*) vznikla jako předchůdce standardu 802.11e. Důvodem bylo rychlé rozšiřování služeb citlivých na zpoždění u běžných uživatelů. Síť bez podpory WMM nebo 802.11e není totiž schopna poskytnout a garantovat požadovanou šířku pásma nebo hodnoty zpoždění vhodné např. pro VoIP nebo video. Výhoda WMM spočívá i ve zpětné kompatibilitě. V síti mohou být zařízení s podporou WMM, ale i bez ní. Tyto stanice jsou řazeny do kategorie *best effort*. [2] [22]

Přístupové třídy (AC- *Access Category*)	**Popis**	**Odpovídající značení priorit v 802.1D (dříve 802.1p)**
Hlas	Nejvyšší priorita - vhodné pro VoIP hovor, u kterého je nutné udržovat malé zpoždění, *jitter* apod.	7, 6
Video	Upřednostňuje video přenos před ostatními daty	5, 4
Best effort	Např. prohlížení internetových stránek	0, 3
Ostatní (na pozadí)	Nejnižší priorita – vhodné např. pro přenos dat	1, 2

Tabulka 4-2 Třídy přístupu u WMM [22]

Jednotlivým datům je přidělena jedna ze tříd přístupu (*AC – Access Category*), podle které jsou zařazena do jednotlivých front. Postup je znázorněn na Obrázku 4-3, na němž je zobrazena i stanice bez podpory WMM s jedinou frontou.



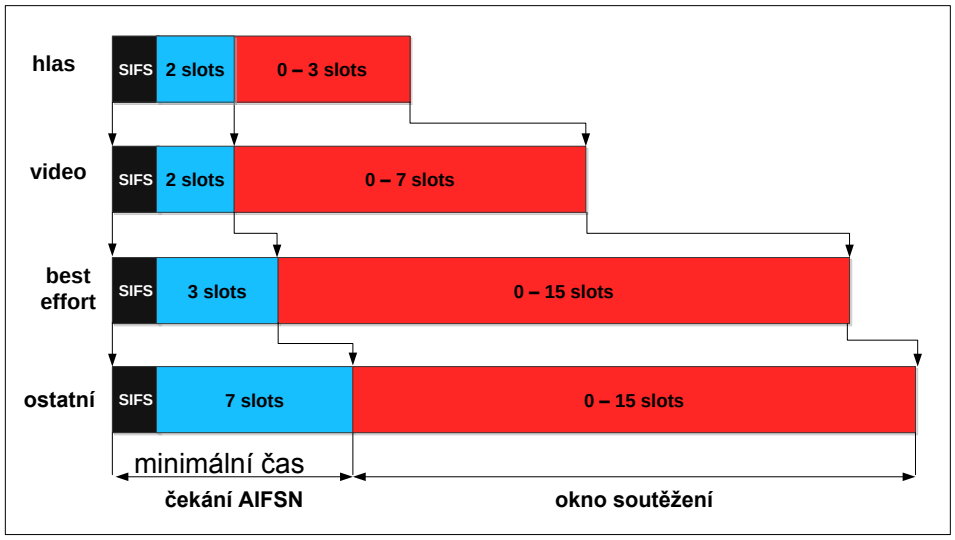
Obrázek 4-3 Rozdělení dat do tříd a do jednotlivých front [7]

WMM vychází z podobných principů jako metoda DCF. Nepracuje ovšem se stejnou dobou čekání DIFS, ale nově vytvořenou dobou AIFS (*Arbitration Inter-Frame Space*). Ta se mění v závislosti na třídě přístupu, čím vyšší priorita, tím kratší AIFS a naopak. Data s vyšší prioritou mají tak vyšší pravděpodobnost, že se rychleji dostanou k vysílání v rámci stanice.

Mezirámcová mezera AIFS se skládá z hodnoty AIFSN (*Arbitration Inter-frame Space Number*) udávané v násobcích *slot time* a mezery SIFS. K této hodnotě se přidává také náhodný interval CW, jenž se mění při vzniku kolize. Její velikost je závislá na třídě přístupu (Obrázek 4-4). Jednotlivé časy, násobky tzv. slotů, jsou u jednotlivých norem různé. Např. délka slotu je 20 µs u standardu 802.11b, g a u standardu 802.11a je to 9µs (Tabulka 4-3).

Data z jednotlivých front přístupových tříd (AC_**) „soutěží“ o tzv. příležitost k přenosu, kterou nazýváme interval TXOP (*Transmission Opportunity*). Výhoda použití intervalu TXOP je v lepší synchronizaci stanic, protože doba, po kterou bude rámec vysílán, je předem známá i ostatním stanicím. Pokud by rámce byly větší než doba trvání intervalu TXOP, budou rozděleny na menší části (fragmenty). Délka intervalu TXOP v normě 802.11a, g je od 0,2 ms (AC_BK) do 3 ms (AC_VI) a od 1,2 ms do 6 ms v normě 802.11b.

WMM poskytuje vyšší pravděpodobnost přidělení větších hodnot šířky pásma pro kategorie s vyšší prioritou při „boji“ o sdílené médium. [16] [22]



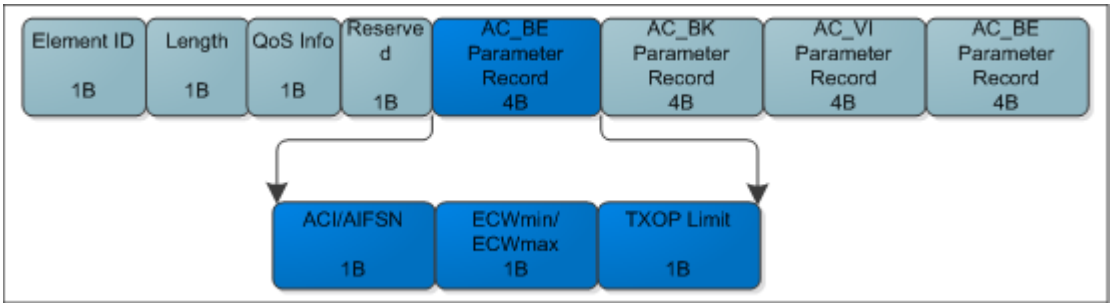
Obrázek 4-4 WMM - jednotlivé časy u tříd přístupu [22]

Mezirámcové mezery, CW	802.11a	802.11b	802.11g	802.11n
SIFS (µs)	16	10	10	16
PIFS (µs)	25	30	30	25
DIFS (µs)	34	50	50	34
CW_{min}	15	31	15	15
CW_{max}	1023	1023	1023	1023
slot time (µs)	9	20	20	9

Tabulka 4-3 Porovnání intervalů a slotů jednotlivých norem

4.2 EDCA (Enhanced Distributed Channel Access)

Tato metoda je rozšíření přístupu k médiu DCF. Ta pracuje se všemi zařízeními se stejnou prioritou – *best effort*. Metoda EDCA rozlišuje provoz a může jednotlivým třídám přiřadit parametry, upřesněné v *beacon* rámci (Obrázek 4-5) a nastavené HC.



Obrázek 4-5 EDCA parametry vyslané v *beacon* rámci [2]

V poli *EDCA Parameters Set* jsou nastaveny parametry (níže uvedeny) pro každou přístupovou třídu zvlášť. V poli *QoS info* se nachází parametr *EDCA Parameter Set Update Count*, kde se zaznamenávají změny EDCA parametrů. Je tedy zajištěno, že stanice poznají změnu parametrů a aktualizují se.

ACI/AIFSN

- AIFSN (4 bit) – počet slotů po mezirámcové mezeře SIFS; kde AIFS[AC] = AIFSN [AC] x aSlotTime + aSIFS
- ACI (2 bit -*AC index*)- hodnota udávající přístupovou třídu – 00-BE, 01-BK, 10-VI, 11-VO

ECWmin/ECWmax

V těchto blocích jsou zakódovány hodnoty CW_{min} a CW_{max}, používané při vytváření intervalu při kolizi v následujícím formátu:

- $CW_{min} = 2^{ECWmin} - 1$
- $CW_{max} = 2^{ECWmax} - 1$

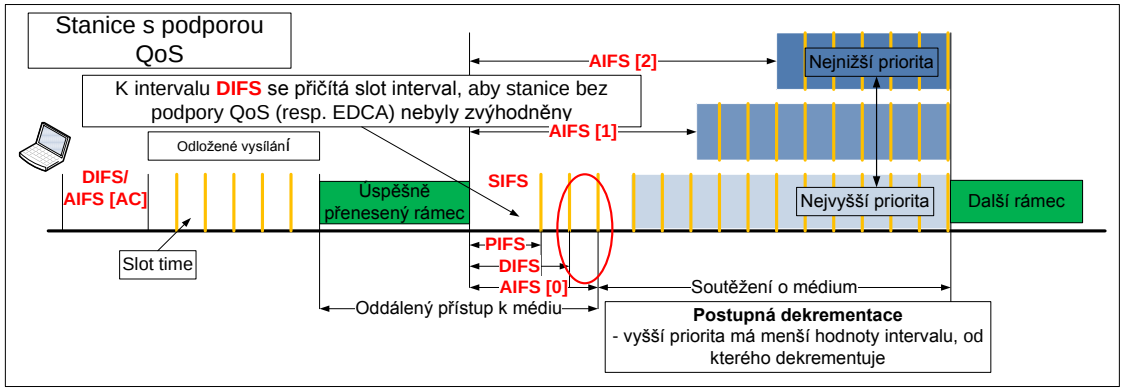
Za zmínku stojí i to, že hodnota CW_{max} vyšší třídy je nižší, než CW_{max} třídy o stupeň níže. Při kolizi má tedy třída o vyšší prioritě zaručenu vyšší pravděpodobnost rychlejšího doručení, avšak na úkor třídy s nižší prioritou, která bude mít odklad vysílání delší. Po úspěšném přenosu se CW vrátí na svou původní úroveň.

TXOP Limit

V tomto poli je uložena maximální hodnota intervalu TXOP. Je udávána v násobcích 32 µs a pro každou třídu přenosu je jiná. V tomto intervalu smí stanice vysílat svá data stejné přístupové třídy a započítávají se do něj i čekací doby SIFS a rámce ACK. Spolu s touto hodnotou je v každém rámci také uložena informace o jeho celkové délce. Ostatní stanice tedy ví, jak dlouho bude vysílání trvat, a podle toho si nastaví svůj interval NAV. To platí v případě nenulové hodnoty TXOP.

Pokud je hodnota TXOP nulová, tak daná kategorie přístupu může odeslat jen jeden rámec. V případě, že je rámec vetší než hodnota TXOP, bude rozdělen. Menší priority přístupových tříd mají TXOP rovno nule, a tak mohou přenést jen jeden rámec. Vyšší priority mají hodnotu větší, a tak můžou přenést více rámců najednou. Viz Obrázek 4-6. [1] [7] [11] [18]

Chce-li vysílat více stanic s provozem o vysoké prioritě najednou (např. VoIP přenos), pak jistou nevýhodou je, že mají-li pakety nejvyšší prioritu, stále se mohou zdržet při kolizích. To je dáno malou hodnotu CW_{max}, která je při kolizích rychle dosažena a stanice tak budou mít nejvyšší možnou dobu odkladu pro svou prioritu. Stále bude však menší než u nižší priority.



Obrázek 4-6 Časový průběh metody EDCA [18]

4.3 HCCA (HCF Controlled Channel Access)

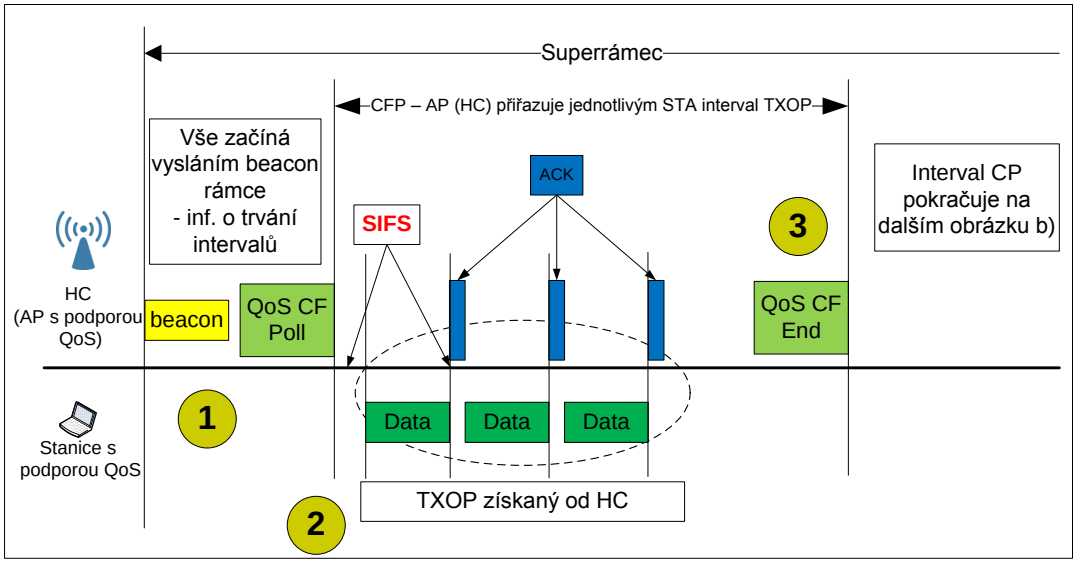
Metoda HCCA vychází z PCF a vylepšuje ji. V původní metodě PCF nebylo možno zaručit vysílání *beacon* rámců ve zcela stejných intervalech. HCCA zavádí podmínku, že žádná stanice nesmí vyslat data, která by přesáhla dobu vysílání následujícího *beacon* rámce. Dalším rozdílem je možnost HC (*Hybrid Coordinator* – nejčastěji AP s podporou 802.11e) přidělit interval TXOP v kterémkoliv bodě průběhu superrámce, zaznamená-li nečinnost v trvání mezirámcové mezery PIFS.

V původní PCF se stanice registrovaly u AP bez požadavků na šířku pásma či služby. AP poté postupně rozesílal rámce CF-Poll během doby bez soutěžení na jednotlivé stanice, mají-li nějaká data k vyslání. HCCA je založeno na podobném principu. Liší se v tom, že stanice posílají své požadavky na síťové prostředky HC. Ten je vyhodnotí, přijme, případně odmítne, není-li schopen tyto požadavky zaručit. Na základě požadovaných síťových prostředků se přiřazuje interval TXOP. Ten je samozřejmě odlišný pro každou třídu priorit.

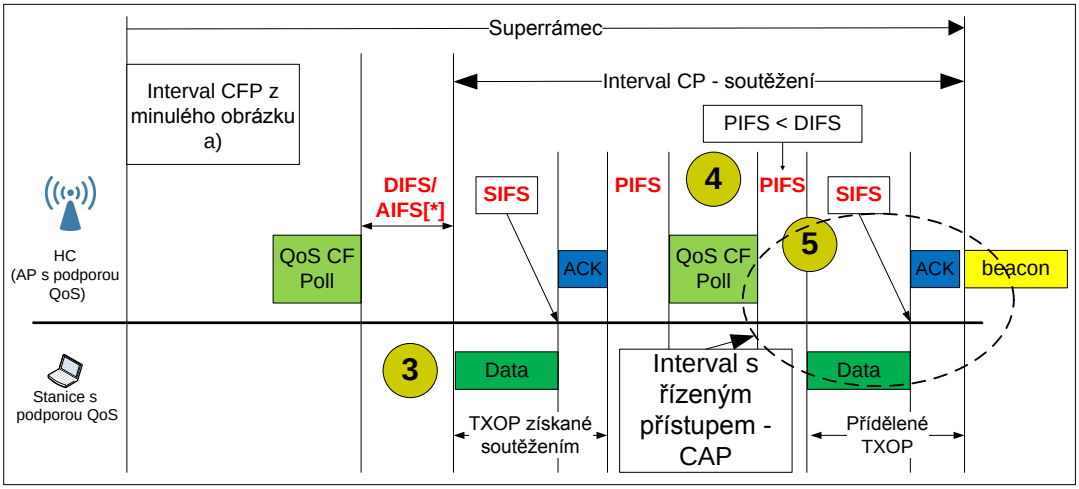
Princip je znázorněn na Obrázku 4-7 a 4-8.

Popis jednotlivých kroků:

1. Interval bez soutěžení CFP začíná odesláním *beacon* rámce, ve kterém jsou upřesňující informace např. o délce intervalů TXOP a CFP.
2. Po odeslání *beacon* rámce vyzve HC stanice prostřednictvím rámce QoS CF-Poll k vyslání dat po dobu trvání intervalu TXOP. Pokud jsou data příliš velká, budou rozdělena do jednotlivých fragmentů.
3. Interval CFP je ukončen vysláním speciálního rámce CF-End. Po něm začíná interval soutěžení - CP.
4. V intervalu CP - stanice, která jako první dekrementuje své generované číslo na 0, obdrží TXOP a může začít vysílat. Limit TXOP je posílán v rámci QoS CF-Poll na rozdíl od metody EDCA, kde je interval TXOP upřesněn v *beacon* rámci.
5. HC může přerušit interval CP a přidělit tak právo vyslat data jiné stanici. Stačí, když po vyslaném rámci počká dobu PIFS (ta je kratší než DIFS) a vyšle QoS CF-Poll. Doba trvání TXOP v intervalu CP se nazývá interval s řízeným přístupem (CAP - *Controlled Access Phase*). [1] [11] [14] [18]



Obrázek 4-7 Metoda HCCA a) [18]



Obrázek 4-8 Metoda HCCA b) [18]

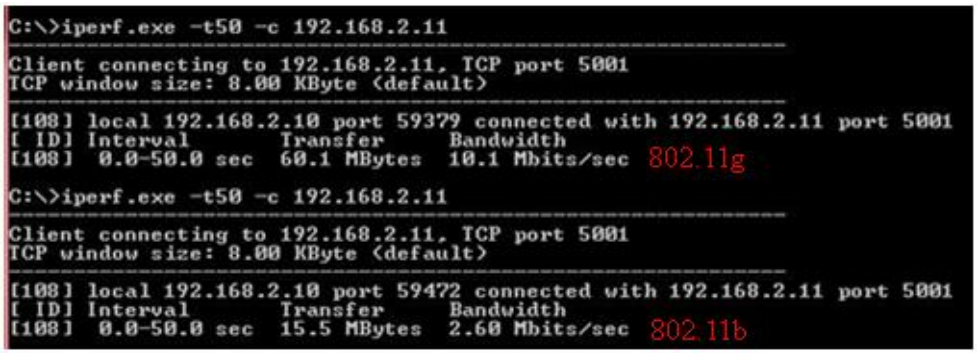
5 WMM v praxi

Testovací souprava:

- notebook Sony VAIO VGN-NR31Z/S s WiFi kartou Intel 4965AGN s podporou technologie WMM
- stolní počítač
- notebook Asus F5N
- směrovač Asus WL-520GC – nejdostupnější typ s podporou WMM
- 2x USB WiFi karta Airlive WN-200USB s podporou WMM
- 2xUSB kamera CNR-WCAM813

Pro testování byla vytvořena bezdrátová síť „Pokus“ se zapnutým šifrováním WPA2-PSK a s pomalejším standardem 802.11b. Ten byl použit proto, aby byla síť co nejvíce vytížena.

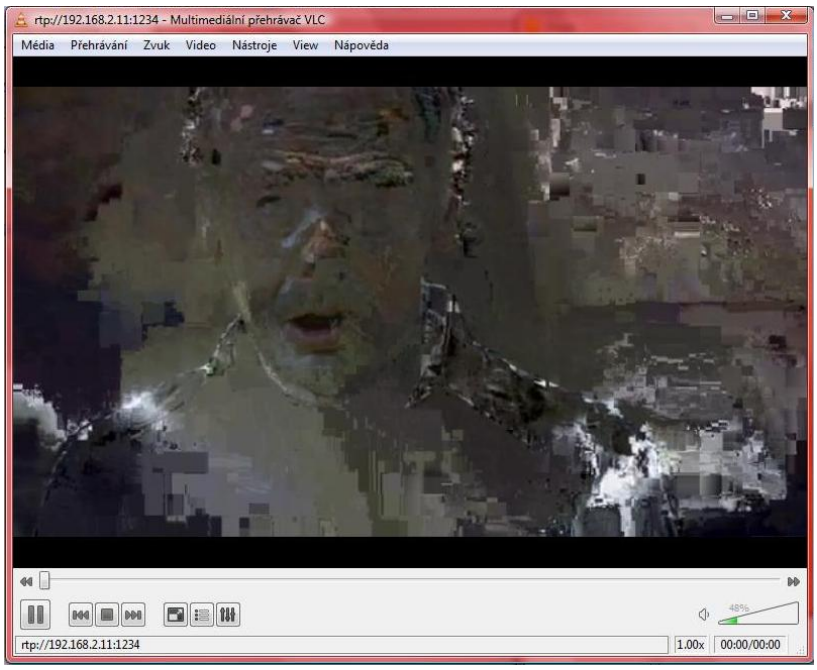
Propustnost nezatížené sítě byla proměřena programem IPerf, který je volně dostupný například z adresy http://IPerf.sourceforge.net. Na Obrázku 5-1 jsou zaznamenány výstupy z tohoto programu pro porovnání hodnot ze standardu 802.11b a 802.11g. Zkouška videohovoru pomocí programu X-Lite byla plynulá a hovor srozumitelný. Proudové vysílání videa pomocí programu VLC media player bylo bez trhání obrazu či jiných chyb.



Obrázek 5-1 Test propustnosti sítě pomocí IPerf

Pozn. Propustnost sítě 802.11b bez zapnutého WPA2 byla o něco vyšší – 2.69 Mbit/s (test byl proveden také programem IPerf).

Test propustnosti byl prováděn na vzdálenost cca 10 metrů přes dvě panelové zdi. Po vyhledání okolních sítí byl zvolen kanál č. 1, aby bylo možné minimalizovat okolní rušení.



Obrázek 5-2 Chyby při přehrávání videa programem VLC v zatížené síti

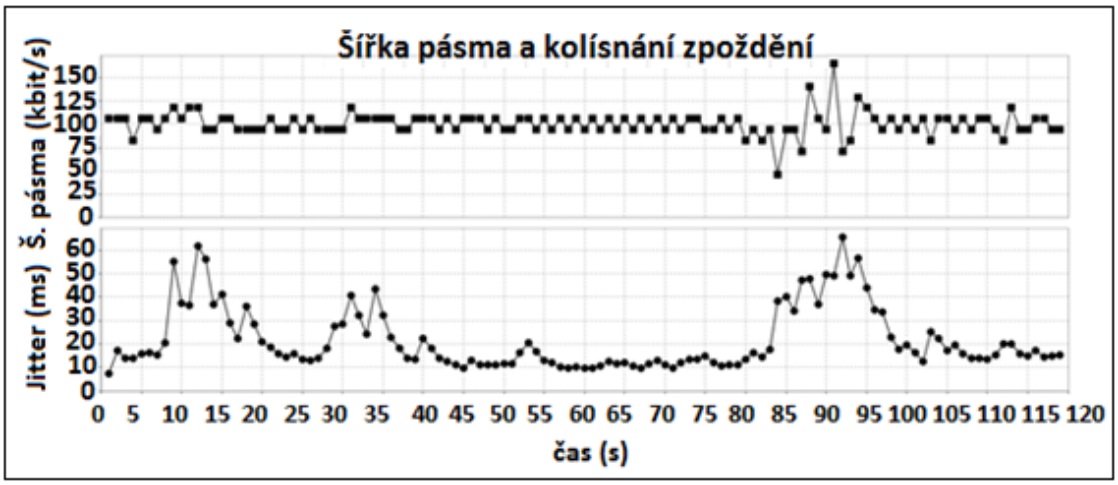
Na počítači č. 1 běžel program IPerf 2.0.2, který využíval protokol UDP jako simulaci VoIP, využívající šířku pásma 100 kbit/s (cca 12.5 kB/s). Šířka pásma byla úmyslně zvětšena pro vyšší zatížení sítě. Standardní rychlost VoIP se pohybuje kolem 8 kB/s a videohovor okolo 43 – 63 kB/s, hodnoty byly získány z programu Netlimiter při spuštěném programu X-Lite (kodek G.711 pro zvuk a H.263+ pro video). Na počítači č. 1 byl také spuštěn FTP server a program VLC media player, který vysílal do sítě video o datovém toku 1440 kbit/s (cca 180 kB/s). Počítač č. 2 generoval dotazy programem HTTP generátor na webový server spuštěný na počítači č. 3 – program USB Webserver. Počítače č. 2 a č. 3 stahovaly data z FTP serveru. Během zátěže běžel také program Ping, který měřil zpoždění mezi počítačem č. 1 a č. 3. Výsledky jsou uvedeny v Tabulce 5-1.

V nezatížené síti byl videohovor kvalitní a bez sebemenšího problému. Výsledky měření jsou zobrazeny v grafu na Obrázku 5-3. Na grafu je také vidět mírné zakolísání na dvou místech, které je pravděpodobně způsobeno mírným rušením.

		nezatížená síť	zatížená síť	
			bez WMM	s WMM
Ping [ms] 120 dotazů	Min	2	250	2
	Max	38	2658	80
	Průměrná hodnota	13	836	34
	Ztrátovost paketů	0%	5%	1%
Jitter [ms]	Min	4	8	3
	Max	30	67	19
	Průměrná hodnota	12	26	14

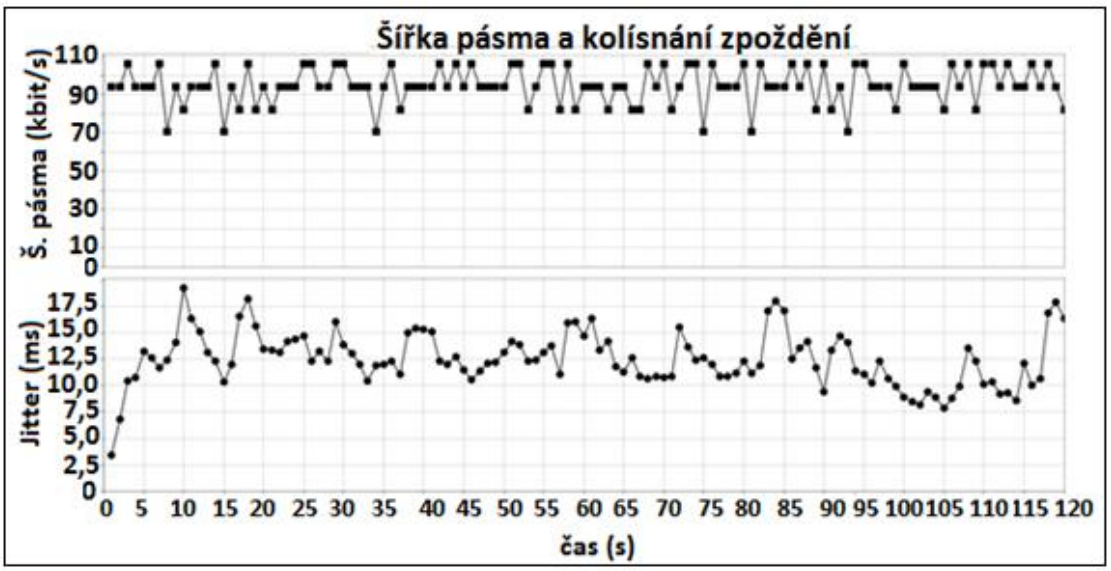
Tabulka 5-1 Zpoždění zjištěné programem Ping a IPerf

Obrázek 5-3 Generování provozu programem IPerf v nezatížené síti



Obrázek 5-4 Zatížená síť bez WMM

Při zatížení sítě vzrostlo i zpoždění měřené programem Ping z průměrné hodnoty 12 na 24. Což by podle doporučených hodnot nemělo činit žádné potíže. Problémem však bylo zvýšení ztrátovosti, která se zvětšila téměř na 5%. Na videohovoru se toto projevilo trháním obrazu.



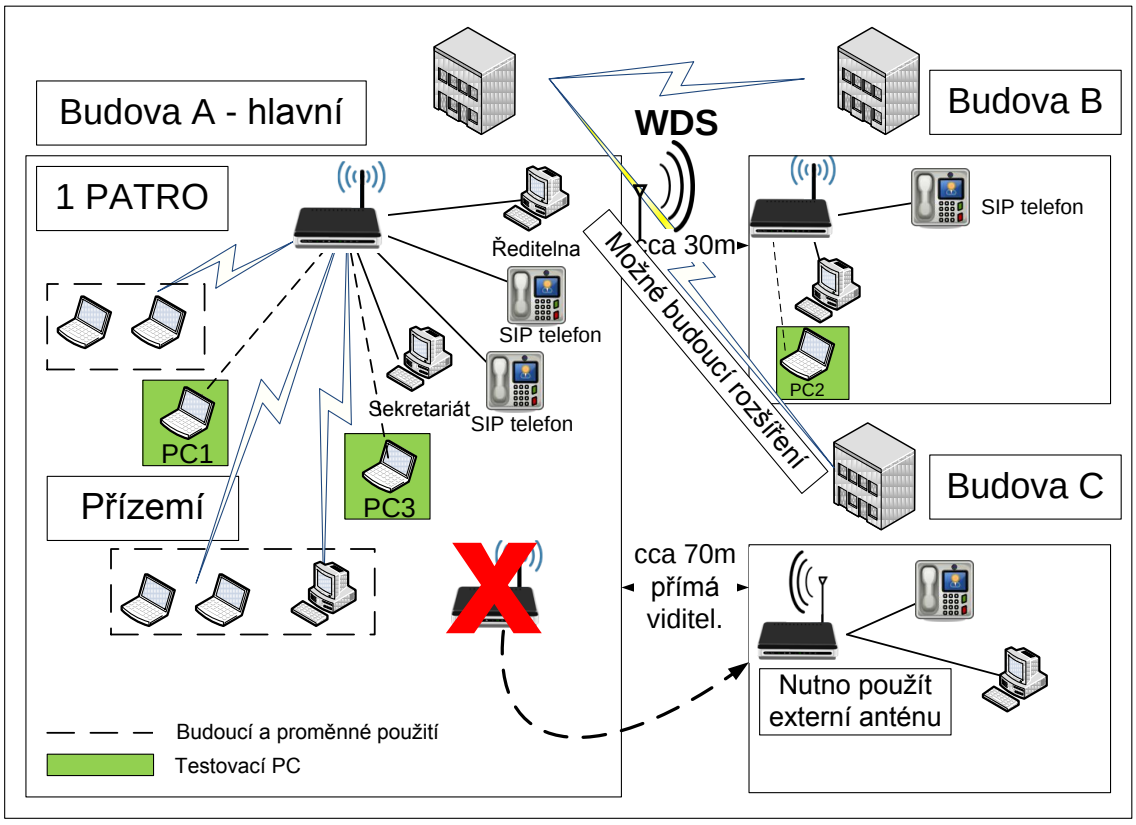
Obrázek 5-5 Zatížená síť s WMM

Při zapnutí služby WMM se velikost parametru kolísání zpoždění, zpoždění i ztrátovost zmenšila. Bohužel v rámci této malé sítě nejsou rozdíly tak veliké. Subjektivně lze ale výsledek ohodnotit tak, že WMM přispěla ke zkvalitnění videohovoru v zatížené síti. Videohovor bylo možno vést bez problémů i v zatížené síti (FTP, prohlížení webu apod.), ovšem za cenu omezení provozu s nižší prioritou.

6 Návrh a realizace sítě

Bezdrátová síť byla vytvořena na půdě školy Acorn's & John's school s.r.o. v Přerově, na základě těchto požadavků:

- pokrytí části přízemí, prvního patra hlavní budovy a přilehlé budovy
- možnost rozmístění interních telefonů (nyní je telefon jen na hlavní budově)
- možnost internetového připojení v jednotlivých třídách (nyní je využíváno pouze pro přístup na internet, avšak v budoucnu bude využíván i tzv. e-learning)
- možnost jednoduchého rozšíření - v průběhu roku budou zakoupeny čtyři další notebooky
- nízké pořizovací náklady



Obrázek 6-1 Návrh a realizace sítě

Při prvním návrhu byly použity tři směrovače TP Link TL-WR543G (802.11b, g), tři VoIP telefony D-Link DPH-120S (SIP protokol) a tři počítače. Plán rozmístění směrovačů byl zvolen v závislosti na dobrém pokrytí požadovaných oblastí. Dva

v budově A – na každém patře jeden a poslední v budově B. Tato konfigurace se ovšem neosvědčila z důvodu velkého rušení (směrovače automaticky použily standard 802.11b s RTS/CTS, při vynucení 802.11g se spojení vůbec neuskutečnilo). Síť byla sestavena, spojení bylo stabilní, ale rychlost celé sítě klesla na ne příliš použitelných 60 kB/s. Konferenční hovor VoIP uskutečněný ze všech telefonů byl subjektivně hodnocen jako kvalitní, ale pro datové spojení je tato rychlost nevyhovující.

U hovoru byl použit kodek G.711, který má kvalitu srovnatelnou s hovorem přes mobilní telefon a jeho přenosová rychlost je asi 64 kbit/s (viz Tabulka 6-1). Používaný telefon může v případě nízké kapacity sítě automaticky použít i jiné kodeky – G.729, G.723.1. Všechny jmenované kodeky podporuje také použitá softwarová ústředna 3CX.

Pozn. Parametr MOS (tzv. Mean Opinion Score) hodnotí kvalitu u VoIP hovoru škálou hodnocení 1 až 5, kdy 1 je nejhorší a 5 nejlepší kvalita hovoru).

Kodek	Algoritmus	Šířka pásma (Kb/s)	MOS
G.711	PCM	64	4.1
G.726	ADPCM	32	3.85
G.728	LD-CELP	16	3.61
G.729A	CS-ACELP	8	3,7
G.729	CS-ACELP	8	3.92
G.723.1	MP-MLQ	6.3	3.9
G.723.1	ACELP	5.3	3,65

Tabulka 6-1 Porovnání jednotlivých kodeků [21]

Problém se nepodařilo odstranit regulací výkonu jednotlivých směrovačů ani změnou vysílacího kanálu. Proto byla zvolena možnost použít jen dva směrovače a třetí ponechat na případné rozšíření sítě připojením vzdálenější budovy - C. Vzdálené spojení je možné, jen je nutné použít výkonnější antény.

Výsledné zapojení tedy bylo pozměněno. Směrovač na budově A byl přesunut na jiné místo tak, aby mohl pokrýt prostor ředitelny a tříd na prvním patře a zároveň zbylé dvě třídy v přízemí. Spojení s budovou B samozřejmě zůstalo zachováno. Samotné propojení směrovačů bylo realizováno pomocí technologie WDS (*Wireless Distribution System*), jelikož požadavkem školy bylo nevyužívat spojení kabelem. To je i hlavní výhoda WDS, možnost vytvořit bezdrátové spojení dvou AP bez nutnosti propojení kabelem. Nevýhodou při tomto použitém propojení je snížení rychlosti sítě, je totiž využíván stejný kanál, na který se připojují i klienti jednotlivých AP. V tomto případě

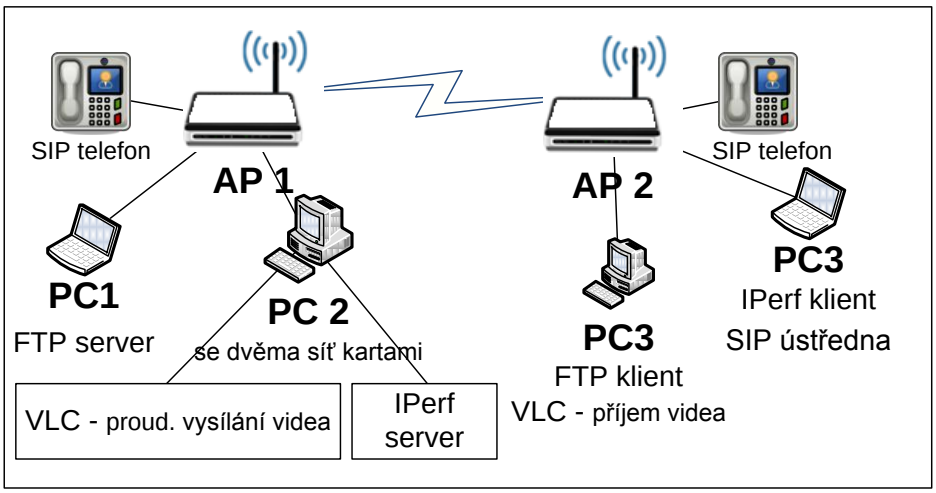
to není na překážku. Jako řešení je možno použít zařízení se dvěma miniPCI sloty – např. MIKROTIK RB532A. Po připočítání dvou miniPCI wifi karet (např. Atheros AR9220 - 802.11n, 2,4Ghz), je celková cena 4300 Kč příliš vysoká.

Původní záměr pracovat jen se zařízeními od firmy TP Link nebyl následně realizován. Důvodem byla absence podpory 802.11e. Směrovače podporovali jen technologie *Port QoS*. Celý projekt musel být upraven a rozdělen do dvou částí. V první je vyzkoušen vliv technologie *Port QoS* na provoz v síti. Ve druhé částí jsou pak použity směrovače Asus WL-520GC, které již podporují technologii WMM.

6.1 TP Link TL-WR543G

Hardware:

- notebook Sony VAIO VGN-NR31Z/S, Asus F5N
- dva stolní počítače
- dva směrovače TP Link TL-WR543G
- dva IP telefony D-Link DPH-120s



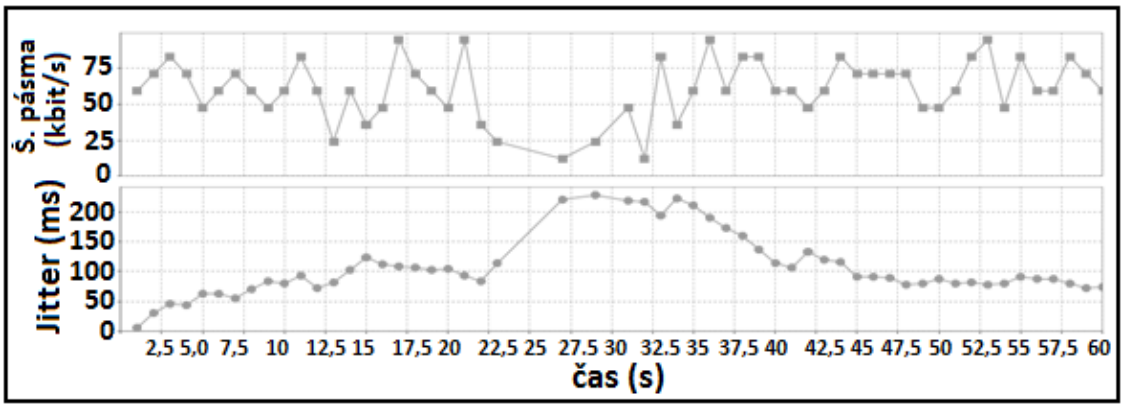
Obrázek 6-1 Síť se směrovači TP-Link

Funkce *Port QoS* se zapíná na směrovačích v záložce *Basic setting/Operation mode*. Umožňuje přidělení pravidel QoS pro jednotlivé porty směrovače, protože rozděluje celkové pásmo poměrově, je nutno nejprve změřit rychlost připojení k síti (popř. internetu) – cca 4 Mbit/s (490 kB/s) pomocí programu NetLimiter.

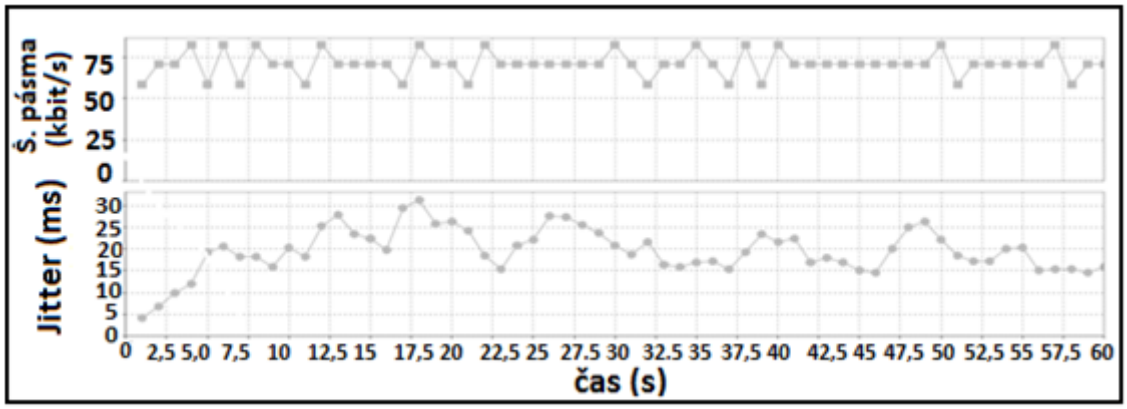
Do portu 1 byl připojen SIP telefon D-Link nevyžadující velkou šířku pásma, proto byla zvolena rychlost 64 kbit/s (8 kB/s) pro oba směry. Rychlost musí být zvolena jako násobek 32 kbit/s. Priorita byla zvolena nejvyšší, aby byly zachovány nejnižší hodnoty zpoždění a jeho kolísání apod. V dalším portu byl připojen počítač použitý pro vysílání videa. Zde je důležité vysílání směrem do sítě. Byla zvolena rychlost 1,5 Mbit/s (47x32 kbit/s), v opačném směru postačí 64 kbit/s. Priorita byla zvolena na druhou nejvyšší, tzn. 1. Na stejném počítači byla nainstalována další síťová karta, v novém rozhraní byl spuštěn program IPerf. Tomuto programu byla nastavena stejné priorita a rychlost jako u VoIP hovoru. Zbývající rychlost byla posléze přidělena FTP serveru na posledním portu. Priorita byla nastavena na číslo 3. Na druhém směrovači, který byl vzdálen cca 30m, byly nastavené hodnoty obdobné jen v opačném směru.

Během testu byl při stahování souboru přes protokol FTP a zároveň při vysílání videa veden VoIP hovor a subjektivně kontrolována jeho kvalita. Hodnoty zpoždění, kolísání zpoždění a ztrátovosti byly měřeny programem IPerf, Ping a následně uloženy ve formě grafů. Z nich je patrný vliv rozdělení provozu pomocí služby *Port QoS*. Při vypnuté službě rychlost vysílání UDP paketů kolísala a v jednom místě došlo i k menšímu výpadku. Pří zapnutí této služby byl provoz s nejvyšší prioritou upřednostněn a jeho rychlost byla udržována jak je vidět na grafu v Obrázku 6-3. Mírné výkyvy jsou způsobeny nejpravděpodobněji rušením z okolních sítí nebo provozem v režimu WDS.

Stručný přehled naměřených hodnot je uveden v Tabulce 6-2.



Obrázek 6-2 Zatížená sít bez zapnuté službou *Port QoS*



Obrázek 6-3 Zatížená sít se zapnutou službou *Port QoS*

Hodnoty z programu IPerf		**Vypnutá služba *Port QoS* zatížená síť**	**Zapnutá služba *Port QoS* zatížená síť**
Rozptyl zpoždění [ms]	**Min**	10	5
	Max	250	33
	Průměrná hodnota	76,46	25,31
Ztrátovost paketů		1,9%	0,6%
Kvalita hovoru - telefon D-Link DPH120S		Hovor byl trhaný a místy nesrozumitelný několika sekundovým výpadkem	Hovor byl v přijatelné telefonní kvalitě

Tabulka 6-2 Shrnutí naměřených hodnot v síti s vypnutou a zapnutou *Port QoS*

V následující tabulce jsou uvedeny doporučené hodnoty pro parametry v síti určujících kvalitu VoIP hovoru.

Parametry	**Hodnoty v síti**		
	Dobré	**Přijatelné**	**Nevyhovující**
Zpoždění	0 – 150ms	150 - 400ms	nad 400ms
Rozptyl zpoždění	0 - 20ms	20 - 50ms	nad 50ms
Ztrátovost paketů	0 – 0,5%	0,5 – 2%	nad 2%

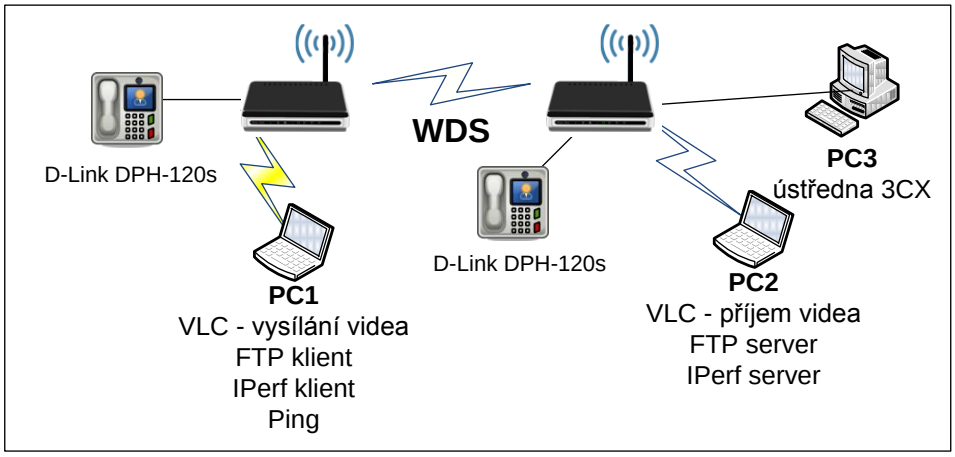
Tabulka 6-3 Doporučené hodnoty pro VoIP [21]

6.2 Asus WL-520GC

Při zkušebním sestavení a testu rychlosti sítě v rámci jedné budovy se naměřená rychlost pohybovala 15,625 Mbit/s (1,9MB/s), test byl proveden pomocí FTP přenosu souboru. Tato rychlost se při rozmístění směrovačů snížila na přijatelných 4 Mbit/s (500 kB/s). Dosažená rychlost je pro naše potřeby dostatečná. Předpokládaná zátěž je jen vedení VoIP komunikace, prohlížení internetových stránek, emailů a do budoucna možnost připojit některé třídy na tzv. e-learning. Zvýšení celkové rychlosti sítě bychom mohli dosáhnout zakoupením směrovačů podporujících novější normu 802.11n s technologií MIMO. Např. směrovač Asus RT-N12, který mimo jiné podporuje i standard 802.11e.

Hardware:

- notebook Sony VAIO VGN-NR31Z/S a Asus F5N
- jeden stolní počítač
- dva směrovače Asus WL-520GC s neoriginálním firmwarem DD-WRT v24 micro
- dva IP telefony D-Link DPH-120s
- 2x USB WiFi karta Airlive WN-200USB s podporou WMM



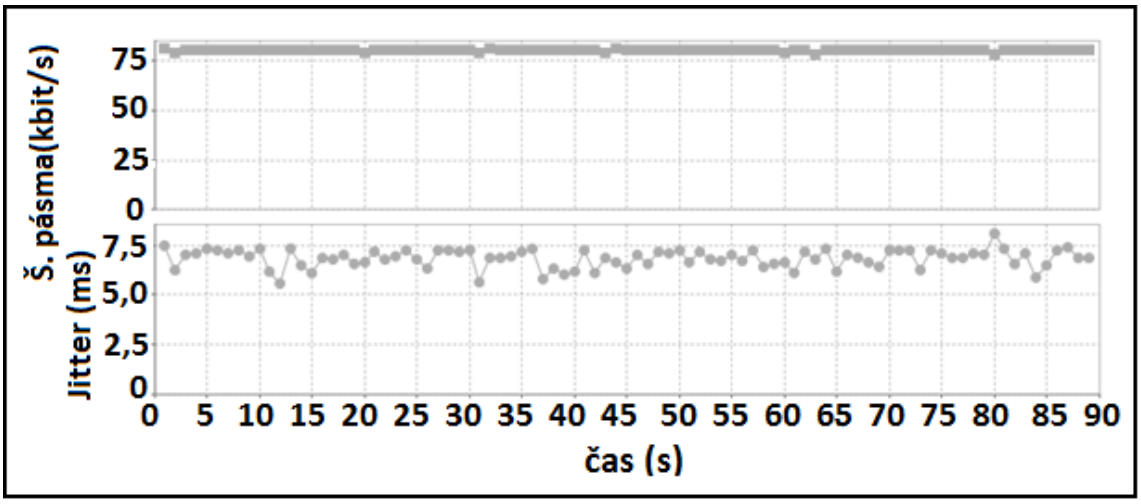
Obrázek 6-4 Testovaná síť se směrovači Asus WL-520GC

Vybavení je obdobné jako v případě předchozího testu. Změnil se pouze použitý operační systém z Windows na Linux – Ubuntu s jádrem 2.6. V tomto systému lze manuálně v jednotlivých aplikacích změnit hodnoty DSCP, které později využívá směrovač při rozlišování provozu, a tím pádem i přiřazení priorit v bezdrátové síti. Další z důvodů byla možnost pozměnit ovladače bezdrátové karty Intel 4965AGN tak,

aby se karta měla možnost přepnout do režimu monitor. Tímto způsobem bylo možno sledovat všechny pakety pomocí programu Wireshark. Počítače byly připojeny k AP pomocí USB WiFi karet Airlive WN-200USB. Jejich ovladač byl stáhnut ze stránek výrobce a zkompilován pro dané jádro. Podpora WMM se zapíná editací konfiguračního souboru nastavením hodnoty „WmmCapable=1“.

Nejprve byla síť podrobena zatížení programem IPerf – protokol UDP s šířkou pásma 71 kbit/s a to příkazem *iperf.exe -c 192.168.2.15 -u -P 1 -i 1 -p 5001 -f k -b 71.0K -t 90 -T 5*. Kde *-c* je režim klienta, *-u* je použitý protokol (UDP), *-P* je počet souběžných datových toků, *-i* je interval zápisů, *-p* je číslo portu, *-f* udává výsledný formát v kbit/s , *-b* je použitá šířka pásma, *-t* je celkový časový interval a *-T* je množství „přeskoků“ (*TimeToLive*). Hovor vedený přes telefon D-Link DPH-120s byl v pořádku. Kvalitu by bylo možno subjektivně přirovnat k hovoru vedenému přes mobilní telefon.

Na Obrázku 6-5 jsou uvedeny výsledky změřené programem IPerf v nezatížené síti při spojení vzdálených směrovačů v budovách A i B technikou WDS. Rychlost vysílání je konstantní, kolísání zpoždění se pohybuje v rozmezí od 5,2 do 7,8ms. Ztrátovost paketů je 0,078% (7 z 9001 paketů).

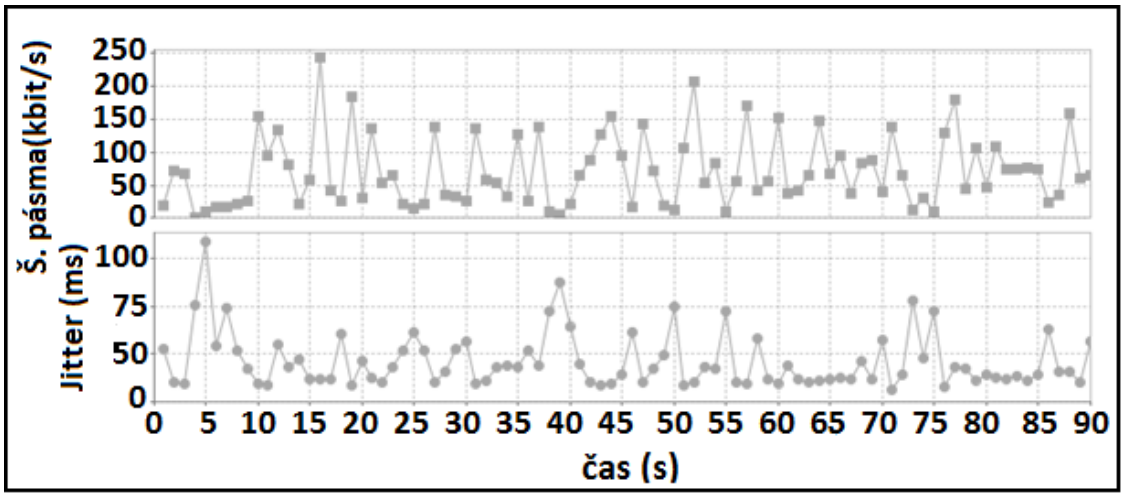


Obrázek 6-5 Bez zátěže a při spojení WDS, IPerf (71 kbit/s)

Dalším krokem bylo zatížení sítě přenosem souboru z FTP serveru a později i vysíláním videa (cca 1,5 Mbit/s, 180 kB/s) v sítí se zapnutou i vypnutou službou WMM.

6.2.1 Vypnutá služba WMM

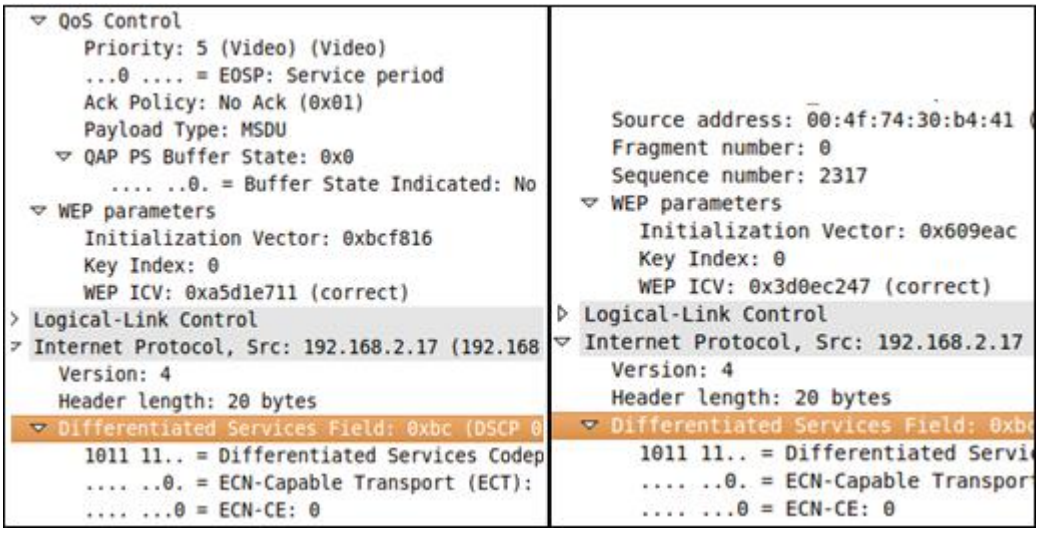
V části testu bez zapnuté WMM byla programem IPerf změřena zatížená síť, a to přenosem souboru pomocí FTP a zároveň vysíláním videa programem VLC. Kvalita hovoru, jak to dokládají hodnoty z programu IPerf, nebyla na přijatelné úrovni. Hovor byl nekvalitní a druhé straně nebylo až na výjimky vůbec možné porozumět. Ztrátovost paketů byla 14% (1260 z 9000). To lze vidět i v první části grafu na Obrázku 6-6, kde UDP pakety vůbec na IPerf server nepřicházejí. Hodnota vysílání UDP paketů nebyla konstantní a stále kolísala od nulových hodnot do 250 kbit/s. Kolísání je způsobeno čekáním dat ve frontách ve směrovači a jejich průběžným zaplňováním a zahazováním, kdy některé z nich vůbec nepřišly na serverovou část programu IPerf.



Obrázek 6-6 Zatížená síť bez zapnuté WMM

6.2.2 Zapnutá služba WMM

Po zapnutí služby WMM se ve sledovaných paketech objevilo pole *QoS Control*, kde jsou vysílány např. informace o nutnosti potvrzování nebo velikosti fronty. Tyto hodnoty se mění v závislosti na typu rámce. Na Obrázku 6-7 je zobrazen přenášený datový rámec, kde je v levé části je podpora WMM zapnutá a v pravé vypnutá. Zařazení do určitých tříd je na základě nastavení aplikace nebo hodnoty pole DSCP. Všechny možnosti obsahu pole *QoS Control* jsou vypsány v Tabulce 4-1.

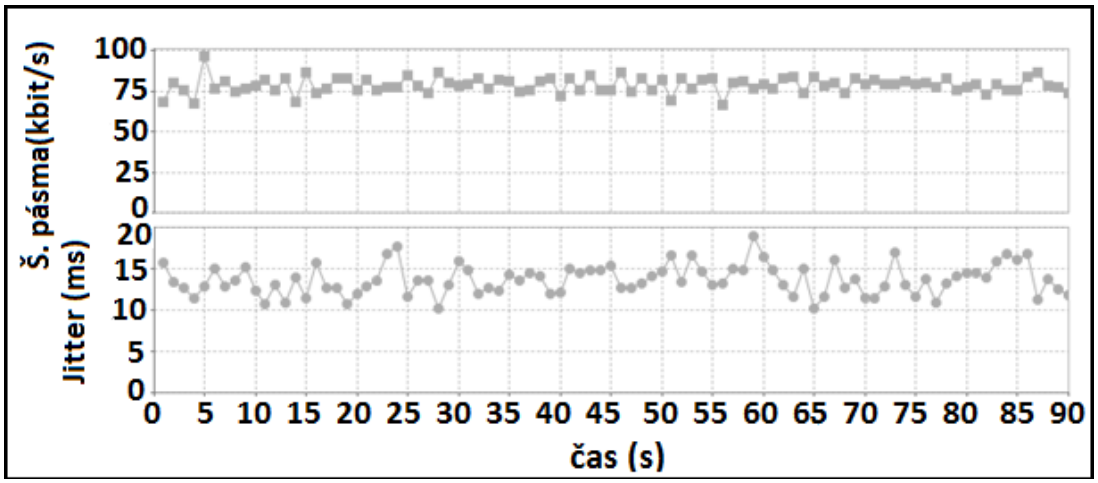


Obrázek 6-7 Pole *QoS Control* v síti se zanutou a vypnutou WMM

Samotné zapnutí služby WMM by bylo nedostatečné. Je nutné nastavit i hodnotu pole DS v jednotlivých aplikací. Nastavení v programu VLC je dostupné z menu nebo lze zapsat do příkazového řádku jako příkaz *--dscp=<celé číslo>*. Při spuštění programu IPerf je nutno přidat parametr *-S <číslo v binární nebo hexadecimální podobě>*. Na měření zpoždění a ztrátovosti byl použit program Ping, jenž kopíroval hodnotu DSCP s programem IPerf. Nastavení programu Ping se provádělo parametrem *-Q <číslo v binární nebo hexadecimální podobě>* a parametrem *-c*, které udává počet ICMP dotazů. V našem případě je tento počet 90.

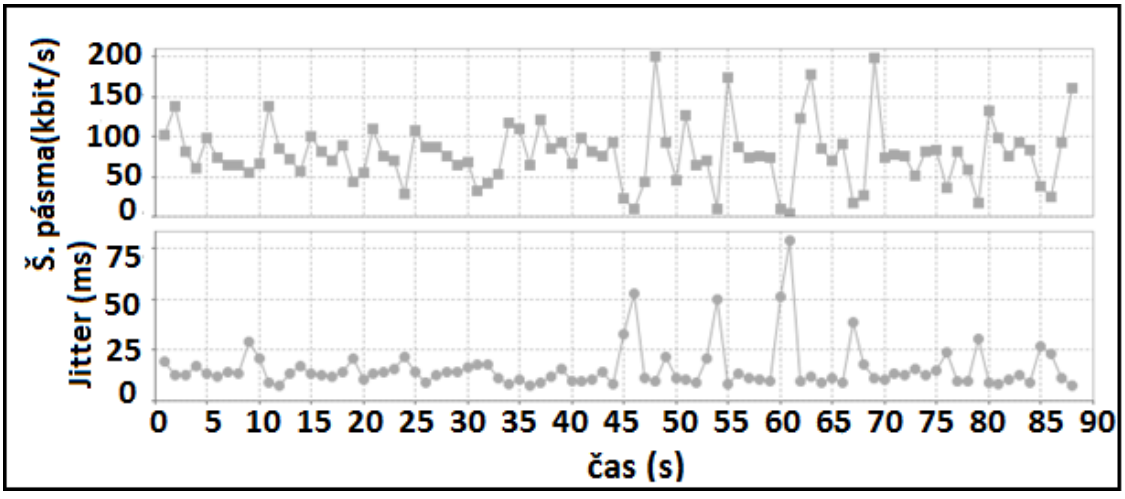
V grafu na Obrázku 6-8 jsou zaznamenány hodnoty při provozu v zatížené síti FTP přenosem, vysíláním videa, hovorem pomocí telefonu a měřením programem IPerf. Hodnota DSCP v programu IPerf a Ping byla nastavena na 0xb8 (decimálně pak 184), což odpovídá přednostnímu zacházení s pakety – jde o Expedited Forwarding (EF). Zacházení EF nabízí záruku velikosti hodnot, jako je kolísání zpoždění, zpoždění apod., pro danou třídu přenosu. Tyto pakety mají nejnižší možnou pravděpodobnost zahození a jsou tak vhodné pro využití u VoIP hovoru. Jistou nevýhodou je neefektivita z důvodu využívání síťových prostředků. Pro video byla nastavena hodnota 0x80 (dec. 128). Nižší priorita není na závadu, neboť při přenosu videa mohou některé pakety vypadnout. Je lepší, když se v důsledku špatného přenosu objeví chyby v obraze, než kdyby se přerušil hovor. Pro přenos souboru byl zvolen přenos *best effort* (BE). BE je základní službou, která negarantuje poskytnutí síťových prostředků, jen se snaží data vyslat nejlepším možným dostupným způsobem. BE je tak vhodné pro nenáročné aplikace jako je např. FTP. Zde není důležité např. zpoždění, ale spíše správnost doručených dat. Programem

Iptraf byl zjištěn pokles rychlosti přenosu souboru přes FTP při zapnutí provozu s vyšší prioritou – video (z 2,5 Mbit/s na zhruba 1,9 Mbit/s). Přenos videa byl na rozdíl od přenosu s vypnutou WMM až na výjimky plynulý a bez chyb. Totéž platí i pro zkušební hovor pomocí SIP telefonů. Hodnoty kolísání zpoždění - 13ms se dostali skoro až na úroveň nezatížené sítě. Ztrátovost paketů se snížila na přijatelných 1,1% (99 z 9000 paketů), a taktéž se snížilo i kolísání při vysílání paketů.



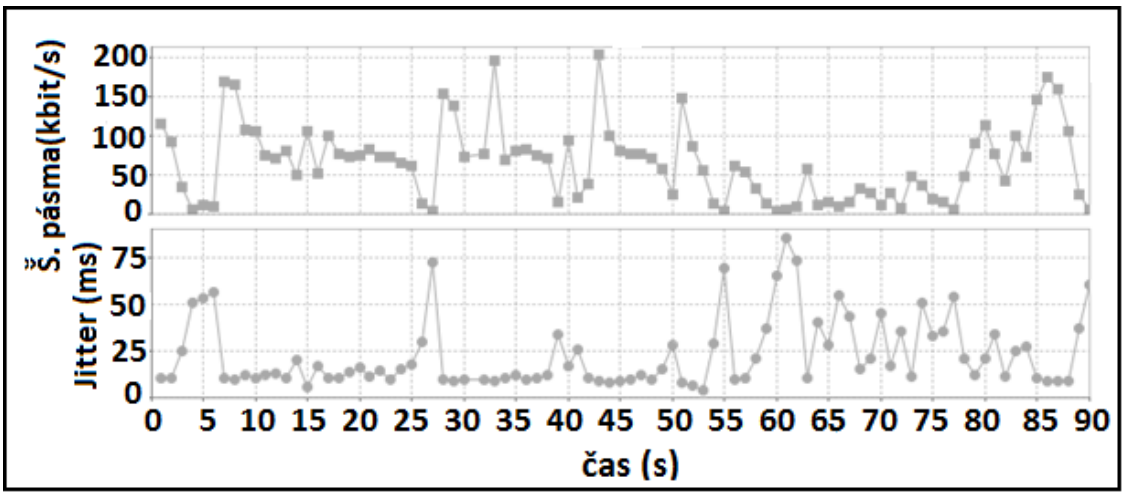
Obrázek 6-8 WMM zapnutá při zatížení sítě

V následujícím grafu je zobrazena situace, kdy byla úmyslně snížena priorita pro program IPerf na hodnotu 0x88. Zacházení paketů se změnilo na Assured Forwarding a zvýšila se i pravděpodobnost zahození paketů. Z nových hodnot je patrno zvýšení sledovaných veličin. Největším rozdílem je zvýšení ztrátovosti téměř na 3%. To je vidět i v pravé části grafu, kde rychlost přenosu několikrát klesla téměř na nulu.



Obrázek 6-9 WMM zapnutá při zatížení sítě, snížená priorita na 0x88

Snižováním priority u programů IPerf a Ping bylo dosaženo dalšího zvýšení ztrátovosti a zvýšení hodnot zpoždění a kolísání zpoždění. Hodnoty ztrátovosti se po snížení priority výrazně navýší skoro na 15%. To je více než v sítí bez zapnutého WMM. Konečné naměřené hodnoty jsou uvedeny pro srovnání v Tabulce 6-4.



Obrázek 6-10 WMM zapnutá při zatížení sítě, snížena priorita 0x80

Nezatížená síť-jen Ping a IPerf			WMM zapnuto			WMM vypnuto
Hodnoty			Zatížená síť	Snížená priorita DSCP 0x88	Snížená priorita DSCP 0x80	Zatížená síť
Zpoždění - Ping 90 dotazů [ms]	min	1,8	43,2	40,7	2,4	3,7
	průměr	2,2	151,8	383,6	490,3	1309,2
	max	4,4	728,8	2181,1	2334,9,1	5486,9
	ztrátovost [%]	0	1	5	15	11
IPerf [ms]	kolísání zpoždění	7,3	12,2	18,6	24	52,8
	ztrátovost [%]	0,13	1,5	3,4	8,2	11
	pakety mimo pořadí	5	54	50	80	25

Tabulka 6-4 Shrnutí výsledků měření

Pro následující provoz celé sítě je důležitý přístup k internetu. Rychlost přístupu k němu byla ověřena v místnostech v prvním patře i přízemí, a také ve vzdálené budově B. Rychlost byla ověřena na serveru www.rychlost.cz . Hodnoty jsou uvedeny

v Tabulce 6-5. Při zjišťování rychlosti internetu byl také proveden hovor na testovací linku poskytovatele VoIP SIPY programem X-Lite. Tato linka je zdarma dostupná na čísle 999 999 499. Nabízí se tak možnost upustit od klasických telefonních linek a přejít kompletně na IP telefonii. V takovém případě by bylo vhodné zakoupit navrhovanou hardwarovou VoIP bránu místo používané softwarové. Použitý kodek byl G.711. U placeného účtu je možnost použít G.729, který sníží použitou šířku pásma a je ve srovnatelné kvalitě.

Místnosti	Rychlost [kbit/s]		Hodnoty zpoždění pomocí programu Ping [ms]			Kvalita hovoru
	Download	Upload	min.	průměrný	max.	
Přímý vstup na internet - Ředitelna	25 375	18 853	11,3	11,5	11,8	Výborná
Třída na prvním patře	16 318	4 091	10,7	10,9	11,4	Výborná
Třída v přízemí	9 168	6 771	27,3	70	116	Výborná
Vzdálená třída v přízemí	5 015	1893	31,8	53,1	89,9	Kvalita poklesla, ale je pořád přijatelná
Vzdálené budova	1 790	449	30,3	44,0	87,6	Přijatelná

Tabulka 6-5 Rychlosti přístupu na internet

Výsledky z grafů potvrzují výhodu technologie WMM, její vliv na snížení kolísání zpoždění a na zpoždění v rámci námi testované sítě. V budoucnu by bylo možno síť rozšířit i na vzdálenější budovu C. V případě připojení by bylo nutno dokoupit externí anténu. Možná cenová kalkulace navrhovaného řešení viz Tabulka 6-6.

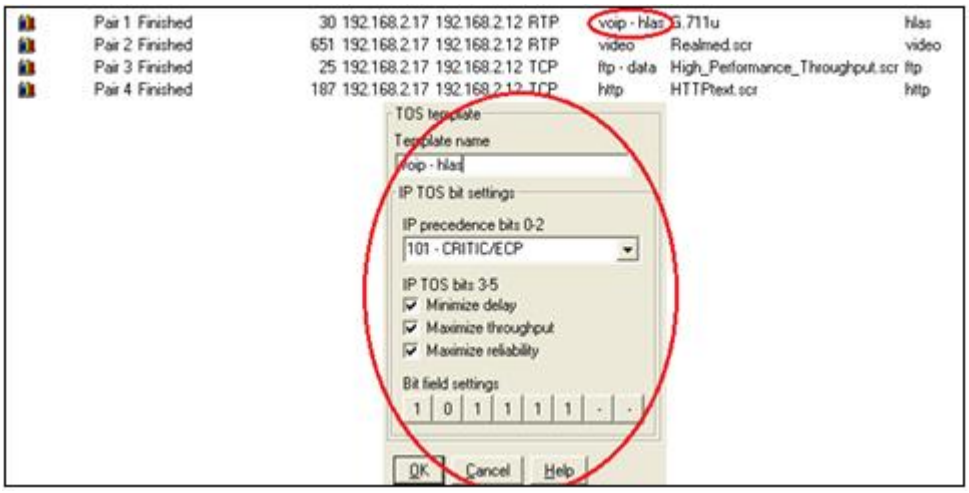
Možnosti	Použitý hardware	Kusů	Cena	Popis/výhody	Celková cena [Kč]
Nynější varianta	Asus WL-520gC	2	1033	-	5957
	OvisLink ePhone-2000s	3	1297	nejlevnější dostupný SIP telefon	
Dražší varianta	ASUS RT-N12	3	1 805	podpora 802.11n,e MIMO	14028
	Cisco SPA502G	3	2 871	větší displej, funkce pro zkvalitnění hovoru	
Možné budoucí rozšíření	Linksys SPA 2102	1	1 987	VoIP brána	1987
	Siemens gigaset C470	x	2 137	bezdrátový VoIP telefon	2137
	PAN-14 PRO	1	775	venkovní panelová anténa	775

Tabulka 6-6 Cenová kalkulace

6.3 IxChariot

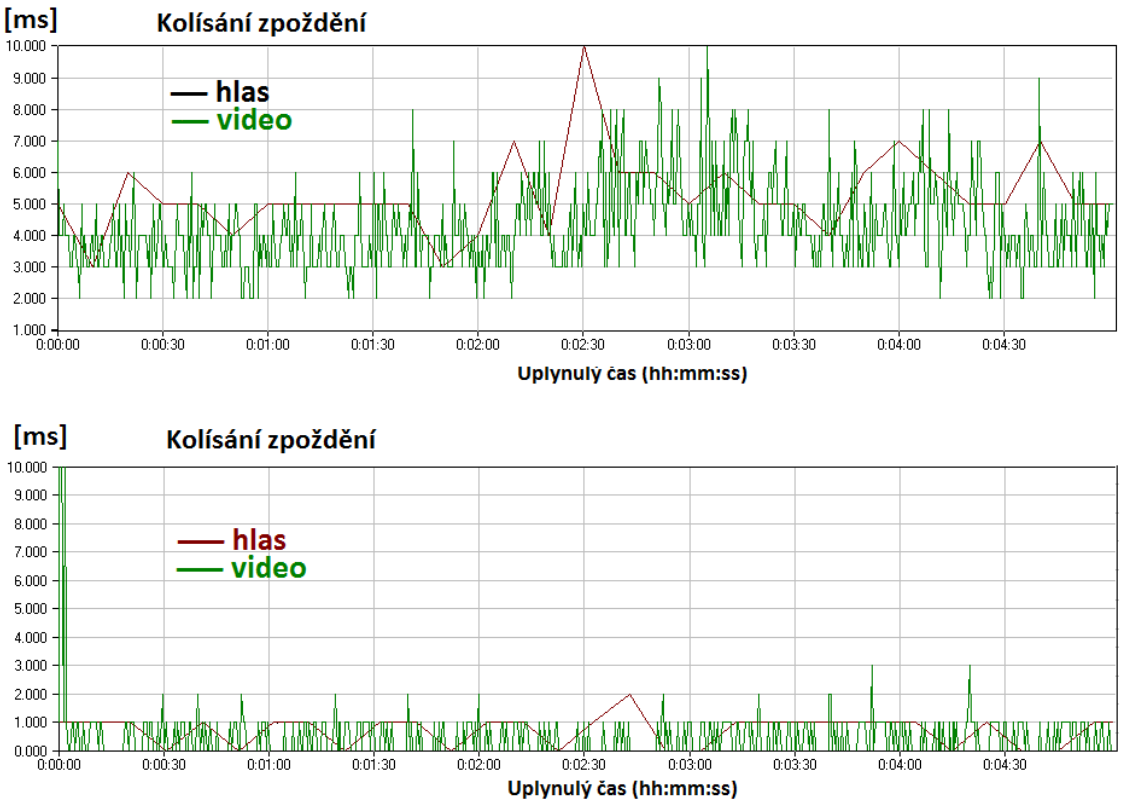
Během práce byl poskytnut na vyzkoušení i program IxChariot od firmy Ixia. V této části práce je ukázáno, jak velký může být rozdíl mezi měřením volně dostupnými prostředky nebo komerčním programem. Vzhledem k jeho ceně musel být test proveden v laboratoři P-249. Směrovače tak byly umístěny v rámci dvou místností přes jednu zeď. V programu je možnost nastavit jednotlivé typy zátěže.

Výběrem „Add Pair…" může být vybrán typ protokolu, ke kterému se přiřadí i skript, jenž určuje typ provozu. V našem případě bylo zvoleno proudové vysílání videa, VoIP hovor, přenos souboru pomocí FTP protokolu a HTTP zátěž, která simuluje prohlížení internetových stránek. Dále byla zvolena jejich priorita (viz Obrázek 6-11; nastavení VoIP hovoru.). Testovaná doba byla 5 minut.

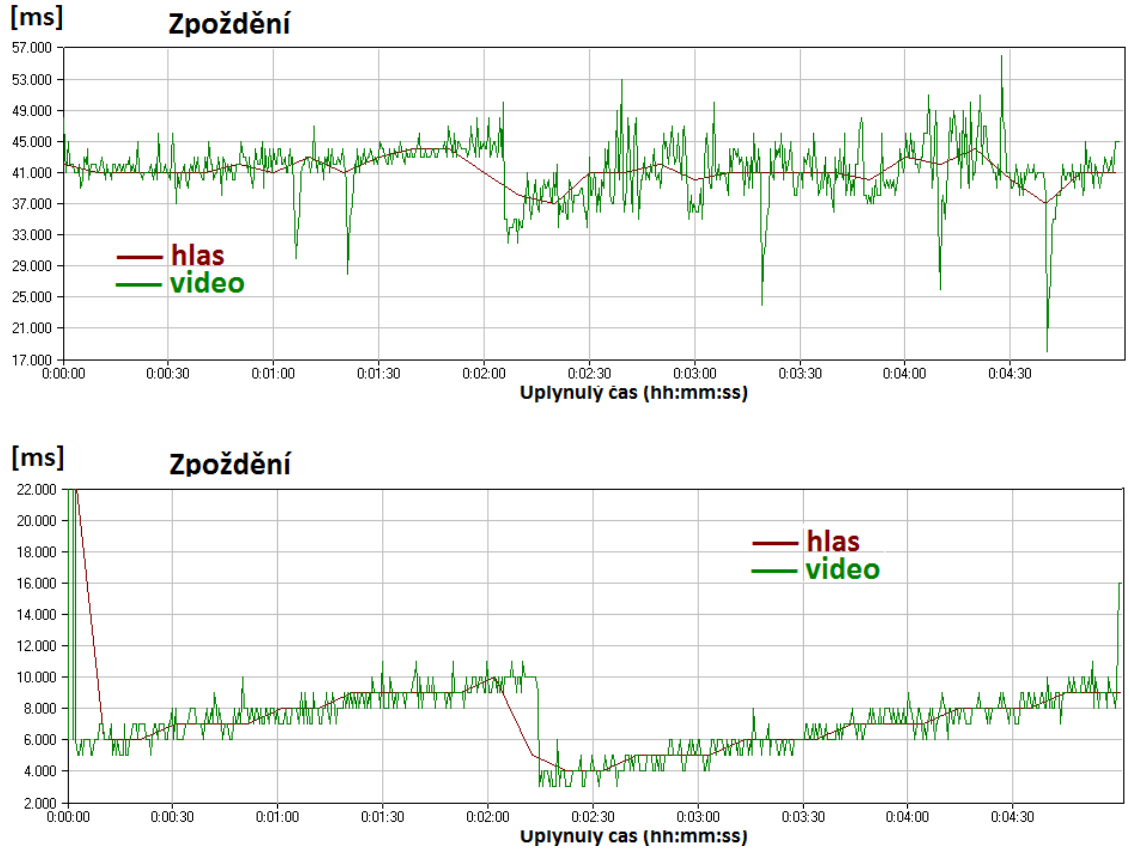


Obrázek 6-11 Nastavení párů a priorit

Na každém počítači musí být nainstalován tzv. Endpoint. Ten lze stáhnout bezplatně ze stránek výrobce a je nutný pro samotné měření. Výsledky měření jsou uvedeny na Obrázcích 6-12 a 6-13.

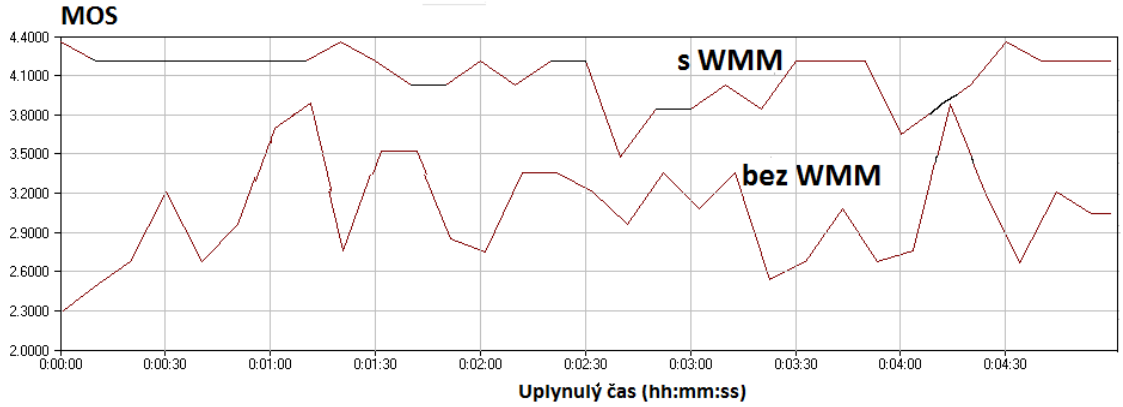


Obrázek 6-12 Kolísání zpoždění s vypnutou/zapnutou službou WMM



Obrázek 6-13 Zpoždění s vypnutou/zapnutou službou WMM

Z grafů lze potvrdit výsledky předcházejících měření. Tedy to, že zapnutá služba WMM na všech směrovačích může pomoci při zkvalitnění VoIP a zároveň i při upřednostnění tohoto provozu, který je tak vysílán rychleji a sníží se u něj hodnoty zpoždění, kolísání zpoždění a ztrátovosti. Posun v kvalitě dokládá i následující graf na Obrázku 6-14. Hodnoty zpoždění a kolísání zpoždění u hlasu a videa mají nastaven rozdíl jen o jednu třídu, proto jsou na grafech vedeny křivky podobně. Výsledné rozdíly jsou uvedeny v Tabulce 6-7.



Obrázek 6-14 Hodnocení kvality VoIP – MOS

Výsledky provedené programem IxChariot tedy potvrdily výhodu zapnuté sužby WMM. Měření na malou vzdálenost však způsobilo, že nejsou mezi hodnotami tak markantní rozdíly. Program dále umožňoval sledovat řadu dalších parametrů, jako jsou např. propustnost, rychlost jednotlivých párů aplikací a ztrátovost dat. Vzhledem k tomu, že rozsah práce je omezen, byly vybrány jen některé z parametrů pro zjišťování kvality sítě pro provoz multimediálních aplikací.

Typ provozu	WMM	Zpoždění [ms]			Kolísání zpoždění [ms]	MOS
		Min	Průměrné	Max		
hlas	vypnutá	37	41	44	5,3	4,1
	zapnutá	4	8	27	0,7	3,06
video	vypnutá	18	41	56	4,3	-
	zapnutá	3	8	209	0,464	-

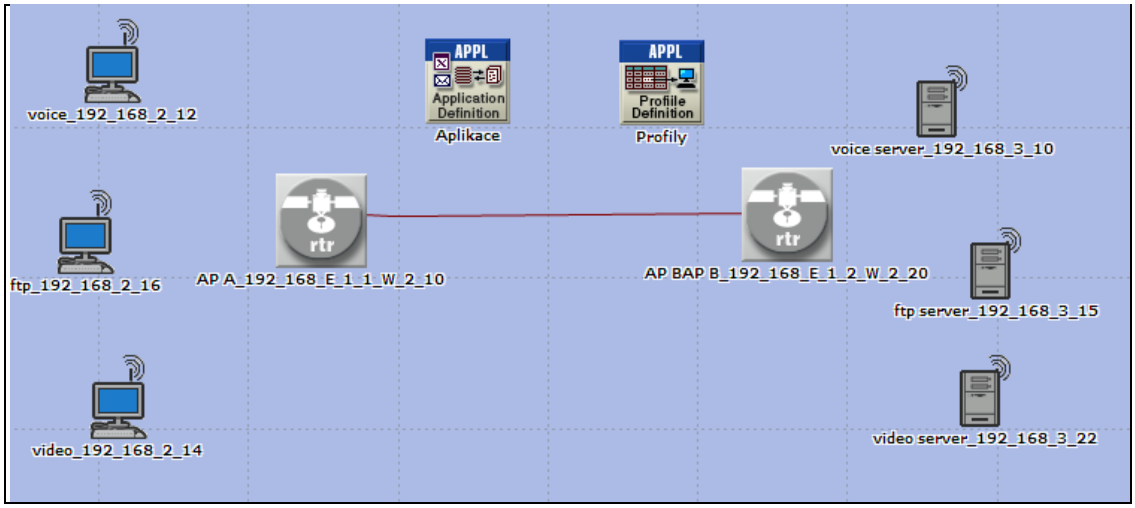
Tabulka 6-7 Výsledné hodnoty z programu IxChariot

6.4 Návrh sítě v prostředí OPNET Modeler 14.5

Program OPNET Modeler usnadňuje práci IT technikům při vytváření nebo pozdějším dolaďování sítí. Někdy je velmi těžké nebo časově nemožné odhadnout v reálném prostředí, jak se firemní síť bude chovat při zátěži. V závěrečné části práce bude vytvořena síť v programu OPNET Modeler, která bude podrobena obdobnému testování. Projekt sítě bude vytvořen ve verzi 14.5. Tato starší verze (nyní existuje 16.0) má určitá omezení týkající se bezdrátových sítí. Např. nefunkčnost WDS (ta je dostupná v novější verzi v doplňku pro bezdrátové sítě - Wireless Suite). [13]

6.4.1 Vytvoření projektu

Projekt se skládá z dvou BSS. První BSS obsahuje tři počítače a každý z nich je určen pro jiný typ provozu. Ke druhé BSS je připojeno stejné množství serverů. Oba směrovače jsou propojeny kabelem *10Base-T*. V kabelu byl definován provoz na pozadí (*Background*) o rychlosti 6 Mbit/s, ten má za úkol omezovat jeho rychlost tak, aby se simulovalo spojení WDS mezi směrovači o rychlosti 4 Mbit/s. Projekt byl vytvořen ve scénáři *Office* a rozměry zvoleny *70x30 m*. Síťové prvky v návrhu jsou *2x wlan_router*, *3x mobile_workstation*, *3x server* poskytující zátěž a objekty pro nastavení aplikací, *application configuration* a *profile configuration*. Síť je zatížena jako v předchozích případech proudovým vysíláním videa, přenosem souboru pomocí protokolu FTP, VoIP hovorem.



Obrázek 6-15 Návrh sítě v prostředí programu OPNET Modeler

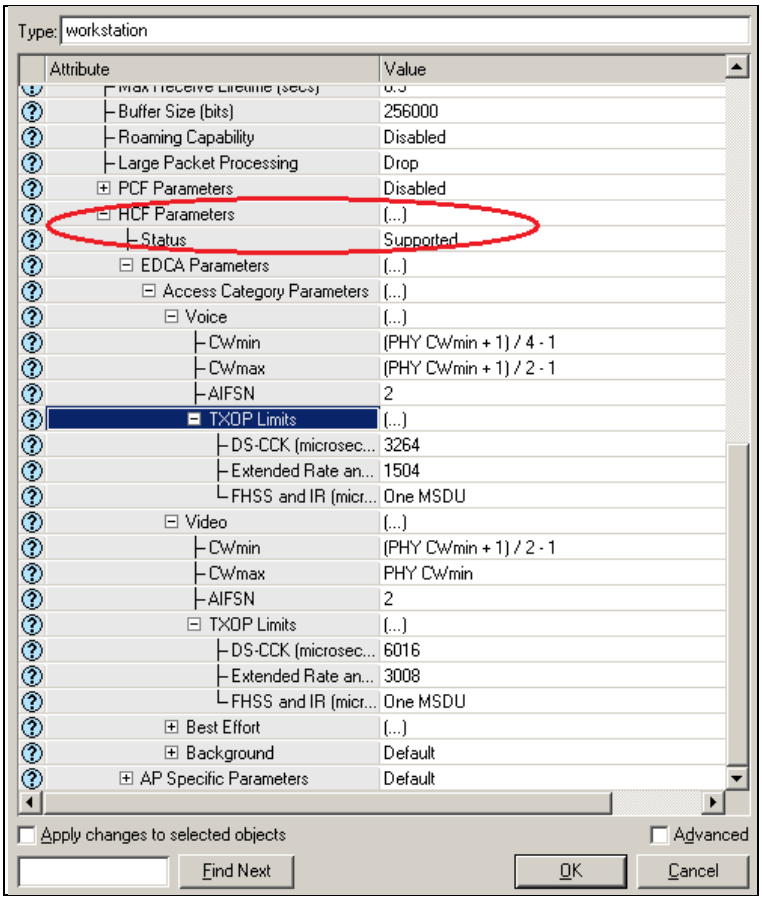
6.4.2 Nastavení parametrů

6.4.2.1 Přístupové body

Z menu *Object palette* byly vybrány dva objekty *wlan_ethernet_router*. Po pojmenování byly nastaveny v menu *Wireless LAN Parameters* tyto parametry - *BSS Identifier: 1* (u druhého směrovače *2*), *Acces Point Functionality: Enable, Physical Characteristics: Direct Sequence (802.11b), Date rate: 11 Mb/s a Channel Settings: 3* (u druhého směrovače *11*). Tímto nastavením jsme zapnuli podporu 802.11b a provozní kanál. Pro zapnutí podpory QoS je nutno mít v menu *HCF Parameters* hodnotu *Enable*.

6.4.2.2 Stanice

Stanice byly přiřazeny k jednotlivým směrovačům změnou hodnoty v menu *BSS Identifier 1* nebo *2*. *Acces Point Functionality* byla vypnutá – *Disable*. *Physical Characteristics* a *Channel Setting* byly nastaveny jako v předchozím případě u přístupových bodů. *Roaming Capability* byla zakázána, protože využívat přesunu od jednoho směrovače ke druhému není v našem případě zapotřebí. Volba *HCF Parameters*, která zapíná podporu pro QoS, byla v prvním testu zapnuta nastavením na hodnotu *default* a ve druhém vypnuta – *Not supported*. V případě nutnosti je v nastavení u stanic možné změnit hodnoty jako je např. velikost okna CW, velikost intervalu TXOP nebo velikost mezirámcové mezery AIFSN. Kdyby tato volba byla vypnuta, stanice by používaly standardní mechanismus DCF bez priorit. Všechny možnosti nastavení jsou uvedeny na Obrázku 6-16. [9]



Obrázek 6-16 Nastavení HCF Parameters

V Tabulce 6-8 jsou uvedeny hodnoty nastavené výrobcem programu OPNET Modeler pro každou přístupovou třídu zvlášť.

Třída přístupu	**Parametry**				
	CW_{min}	**CW_{max}**	**AIFSN**	**Délka intervalu TXOP**	
				802.11 [ms]	**802.11b ,g [ms]**
AC_BK	*CW_{min}	*CW_{max}	7	0**	0**
AC_BE	*CW_{min}	*CW_{max}	3	0**	0**
AC_VI	(*CW_{min} +1)/2-1	*CW_{min}	2	6,016	3,008
AC_VO	(*CW_{min} +1)/4-1	(*CW_{min} +1)/2-1	2	3,264	1,504
* značí hodnotu danou použitým standardem (např. CW_{min} – 15 u 802.11g) ** 0 u TXOP – délka trvání se rovná délce přenosu jednoho rámce					

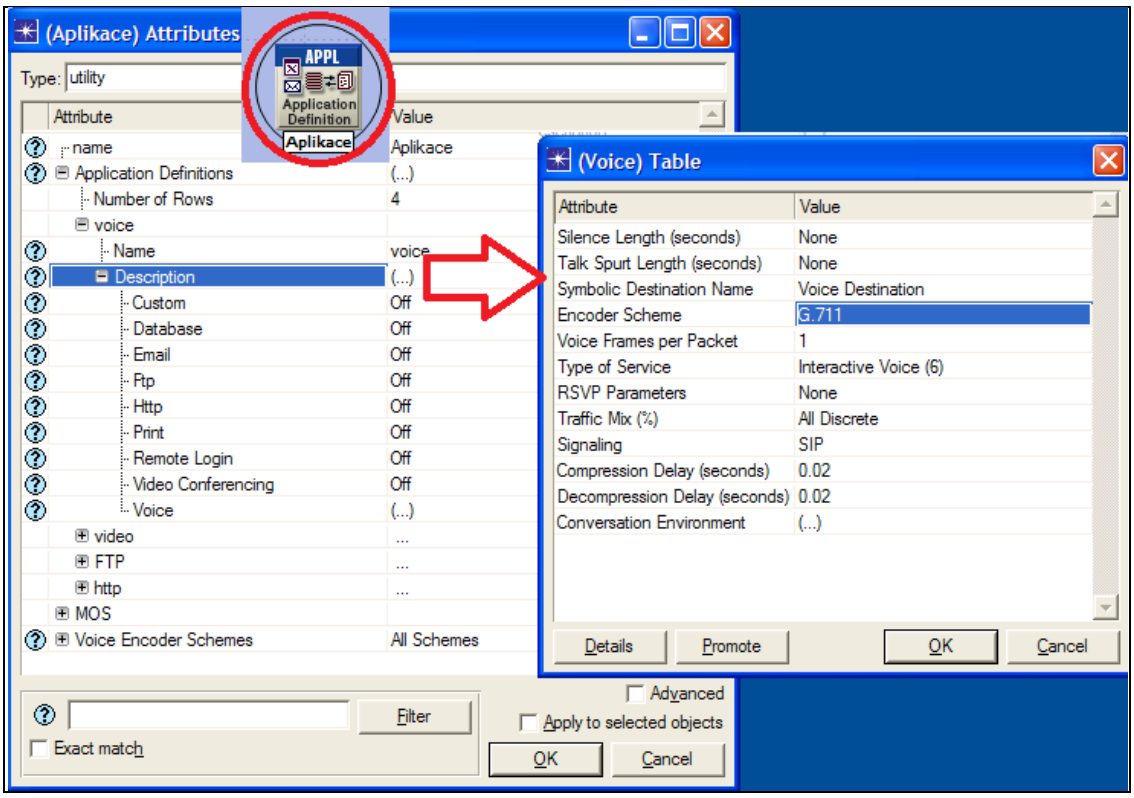
Tabulka 6-8 Standardní nastavení EDCA parametrů [13]

6.4.2.3 Application configuration

K nastavení zátěže je nutno nejdříve jednotlivé aplikace přidat a následně upravit. Vše se nastavuje v prvku application configuration v nabídce zobrazené po zmáčknutí levého tlačítka myši - *Edit Attributes*. Zde zvolíme počet aplikací na tři (*Number of Rows*) a začneme je postupně přidávat.

- VoIP hovor

  Služba byla pojmenována jako Voice. V nastavení byl dále zvolen kodek G.711 a typ služby nastaven na nejvyšší prioritu – *Interactive Voice (6)*. Ostatní hodnoty zůstaly zachovány (Obrázek 6-17).



Obrázek 6-17 Nastavení aplikací v *Application configuration*

- Video

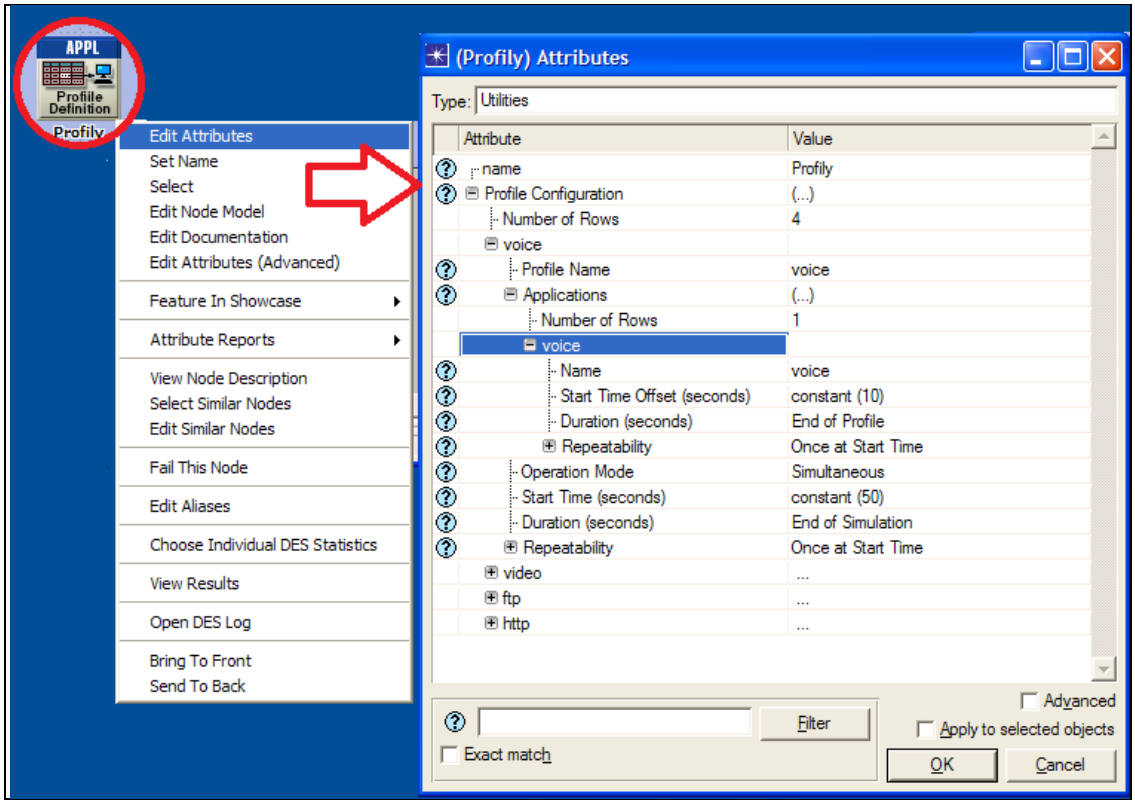
  V nastavení *Edit* byly zvoleny možnosti jako je rychlost snímků *10frame/s*, velikost videa *128x120 pixels* a priorita – *Streaming multimedia (4).* Tímto nastavením bude dosaženo rychlosti cca 1,3 Mbit/s (170 kB/s).

- Přenos souboru pomocí FTP

  V nastavení *Edit* byly zvoleny možnosti – poměr mezi příkazy na server FTP *Command Mix (Get/total): 100%*. Tato možnost zajistí jen stahování souboru ze serveru. Velikost souboru *File Size (bytes): constant (30000000)*, *Inter-Request Time (second): second (120)*, což je časový interval mezi požadavky na server a prioritu – *Best effort (0)*. Přenosová rychlost se bude postupně zvětšovat až na hodnotu okolo 4 Mbit/s (390 kB/s). Pro ukázku je provoz FTP zvýšen zmenšením času mezi zasíláním požadavků na stahování souboru z FTP serveru na hodnotu *40*. První provoz je značen dále v textu jako nízká zátěž a druhý jako zátěž vysoká. [9]

6.4.2.4 Profile configuration

V dalším kroku bylo nutné nastavit chování aplikací. To znamená, kdy se má která aplikace spustit, jak dlouho má běžet, a kdy má skončit, případně se opakovat. Obdobně jako u definování aplikací, navolíme v menu *Number of Rows* číslo 3, stejně jako počet aplikací. Tedy pro každý profil máme jednu aplikaci. Tu přiřadíme k profilu v nabídce *Applications/Enter Application Name*. [9]



Obrázek 6-18 Nastavení chování aplikací v *Profile configuration*

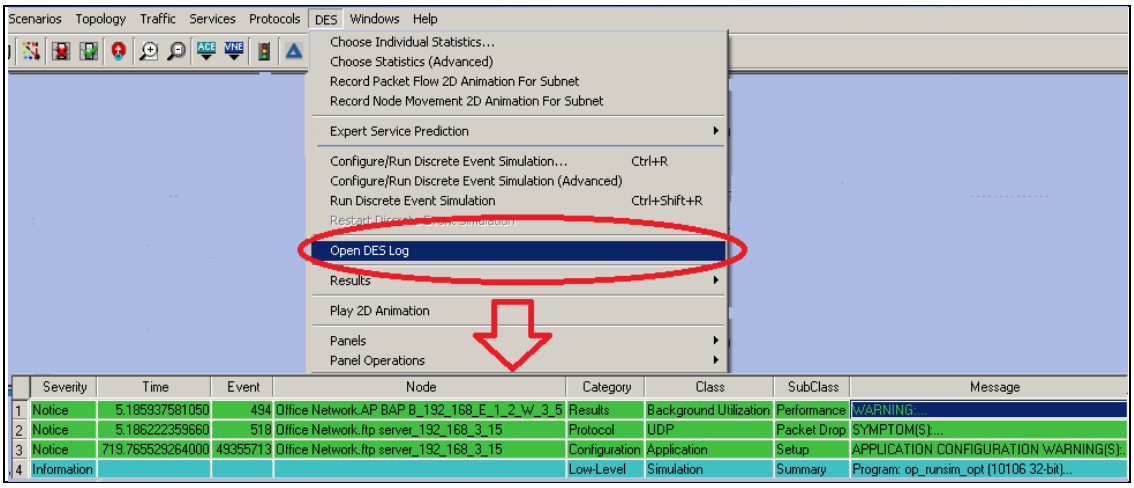
- VoIP hovor

  Telefonní hovor začne 20 s po začátku simulace. Nastavíme *Start time (seconds): constant (10)* a *Start Time Offset (seconds): constant (10).* Trvat bude až do konce simulace – *Duration: end of simulation.* Spouštět se bude společně s ostatními aplikacemi v jednotlivých profilech – *Operation Mode: Simultaneous.*
- Video

  Nastavení videa je obdobné jako v předchozím případě. Jen byl změněn čas spuštění – *Start time offset (seconds): constant (10)* a start profilu *Start time: constant (170)*. Přenos videa se tedy spustí ve třetí minutě simulace. Vysílat se bude 4 minuty - *Duration: 240 (s).*
- Přenos souboru pomocí FTP

  Přenos souboru začne po minutě a půl simulace. *Start time (seconds): uniform (50, 60)* a *Start time: constant (20).* Trvat bude až do konce simulace. Volba *uniform* zaručí spuštění mezi hodnotou 50 až 60 sekund. *Operation Mode: Serial (Order).* Jednotlivé požadavky na server se budou zasílat postupně za sebou. [9]

Ještě než celou simulaci spustíme, musíme přiřadit stanicím v menu *Application: Supported Profiles* profil pro zvolenou aplikaci a v *Application: Destination Preferences* zvolíme server, na který bude provoz směrován. Na straně severu zvolíme jen podporu pro jednotlivé aplikace v menu *Application : Supported Services*. Posledním krokem je nastavení doby trvání simulace – 10min, počet naměřených hodnot – 200 a *update interval* na 10000 událostí. Důležitým parametrem po spuštění a dokončení simulace, který se vyplatí sledovat, je *DES log*, v němž jsou zobrazeny chyby nebo varování. V případě tohoto návrhu zde bylo varování o zahazování paketů vlivem zatížené linky a další chyba je v nastavení aplikace FTP, kdy doba trvání aplikace byla menší než trvání celé simulace.



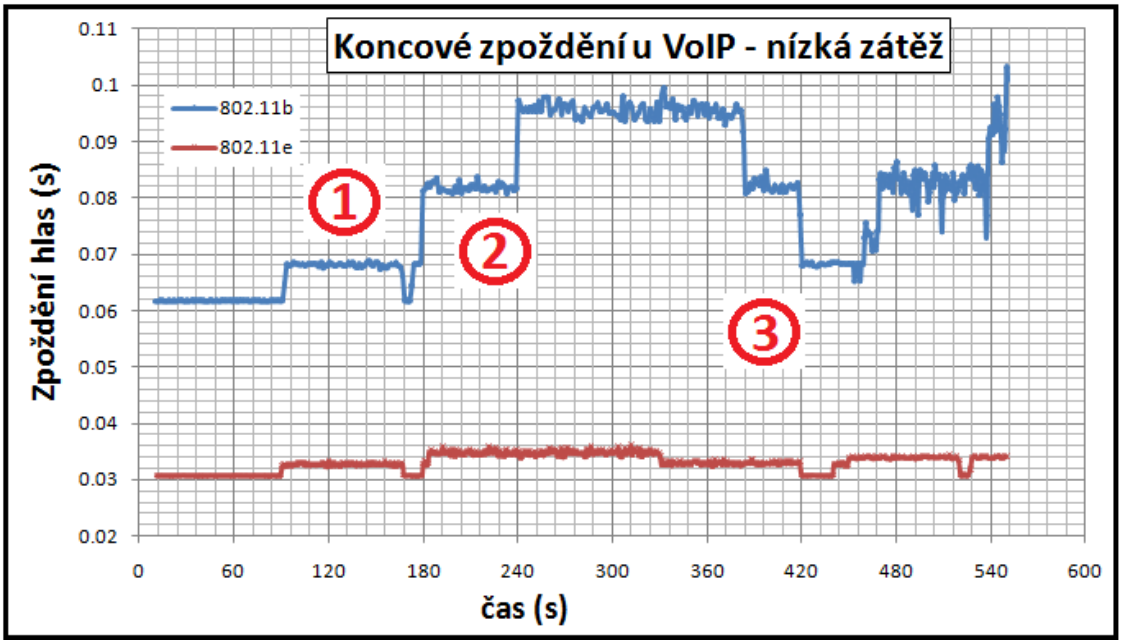
Obrázek 6-19 Výpis menu *DES log*

6.4.3 Výsledky měření

Z široké palety možných měřených hodnot byly vybrány ty, které jsou důležité pro otestování sítě – je-li vhodná pro provoz multimediálních aplikací.

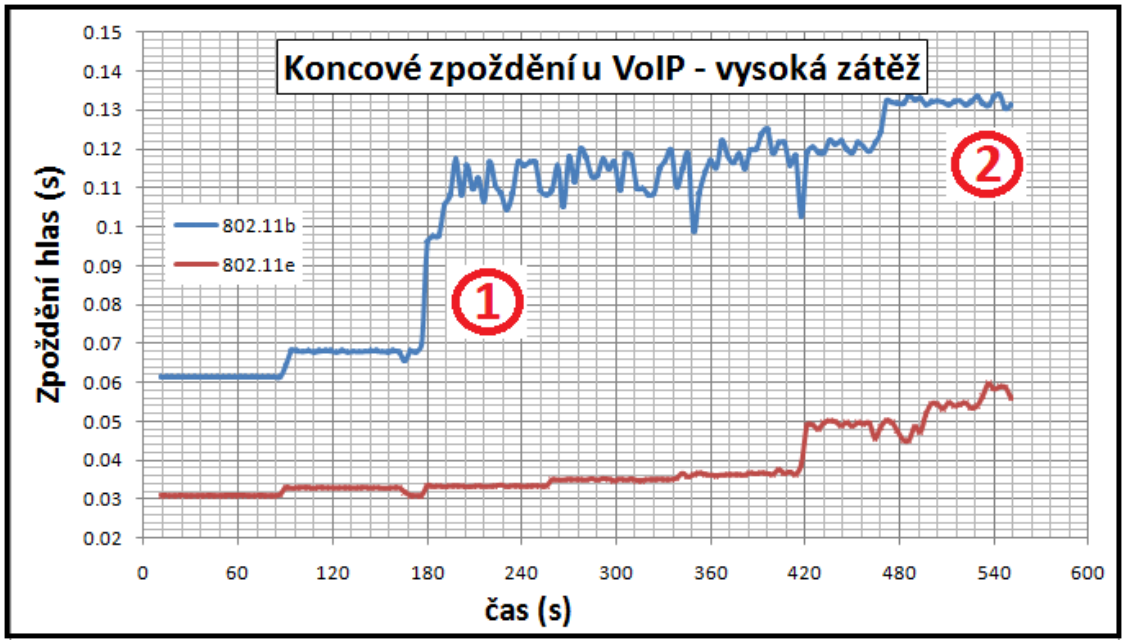
6.4.3.1 Zpoždění

Zpoždění je doba mezi vysláním paketu od zdroje a jeho doručením příjemci. Krajní mez, za kterou je již VoIP hovor nepoužitelný se udává kolem 400 ms. Nárůst zpoždění způsobují např. prodlevy při soutěžení a následné čekání paketů nebo čekání ve frontě na vyslání. Jejich minimalizaci má za úkol snížit právě standard 802.11e. Jeho účinnost při provozu VoIP je znázorněna na Obrázku 6-20. V sítí bez podpory QoS 802.11b se hodnoty zpoždění při každém zapnutí dalšího provozu zvětšují. V bodě 1 byl zapnut přenos souboru a zpoždění se zvětšilo téměř na 70 ms, hodnoty jsou to však stále přijatelné. Opětovné zvětšení nastalo při spuštění vysílání videa a následně dalším požadavkem na FTP server – bod 2. Koncové zpoždění dosáhlo hodnoty 100 ms. V bodě 3 se po vypnutí vysílání videa zpoždění snížilo na úroveň jako před jeho spuštěním. Ke konci simulace se vlivem FTP přenosu opět zvyšuje. V druhé síti jsou změny daleko mírnější. Pohybují se mezi hodnotami kolem 35 ms. To jsou parametry pro VoIP hovor více než dobré.



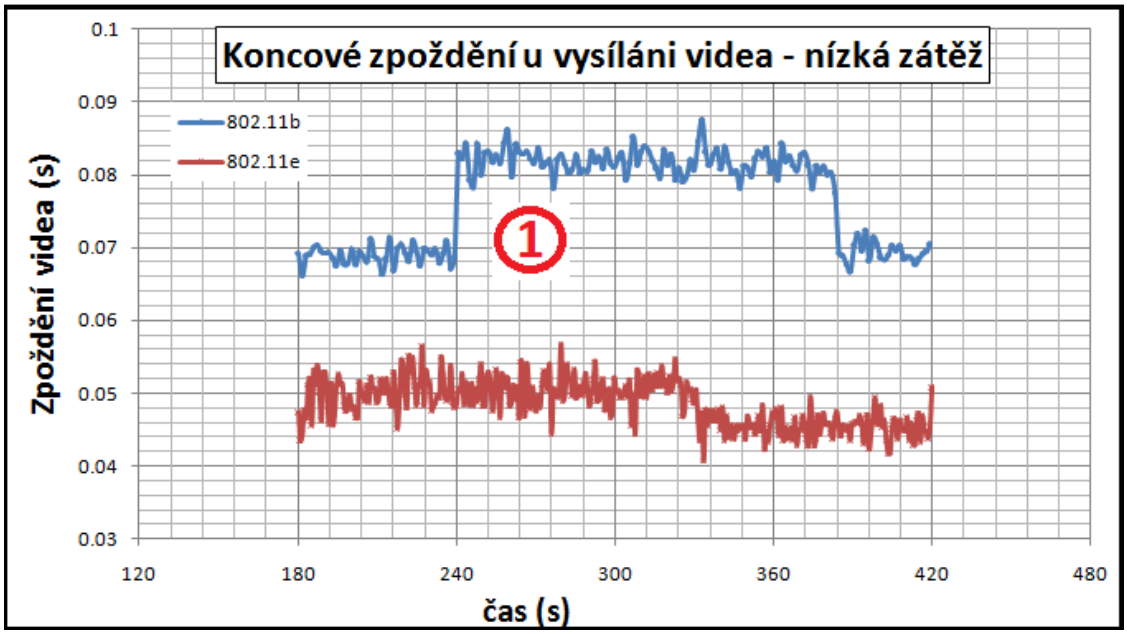
Obrázek 6-20 Koncové zpoždění hlasu v sítích 802.11e a 802.11g

Na následujícím obrázku je zvýšena zátěž. Principy zvětšování jsou stejné jako v předchozím případě. Velký nárůst zpoždění je v bodě 1 při spuštění videa. Maximálních hodnot je dosaženo na konci simulace – u 802.11b - 130 ms a u 802.11e - 60 ms. Nicméně hodnoty pro VoIP hovor jsou stále přijatelné.



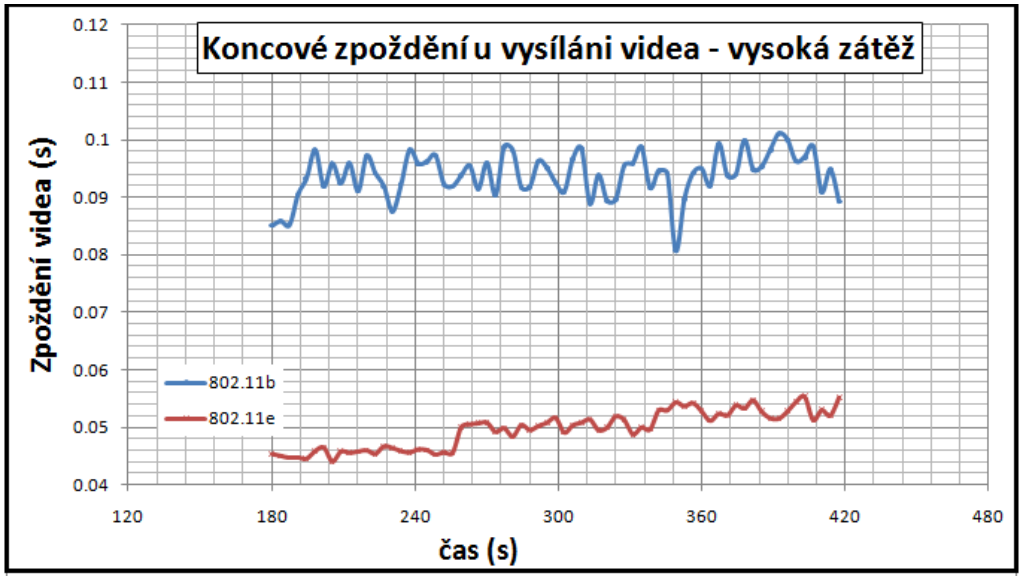
Obrázek 6-21 Koncové zpoždění hlasu v sítích 802.11e a 802.11g

Na dalším Obrázku 6-22 je zobrazeno naměřené zpoždění u videa. Situace je v tomto případě podobná jako u hlasu. Stanice s podporou 802.11e udržuje stále nízké zpoždění na rozdíl od sítě 802.11b, kde hodnoty narůstají. Například při zapnutí FTP se zvětší zpoždění videa až na hodnotu 86 ms – bod 1.



Obrázek 6-22 Koncové zpoždění videa v sítích 802.11e a 802.11b

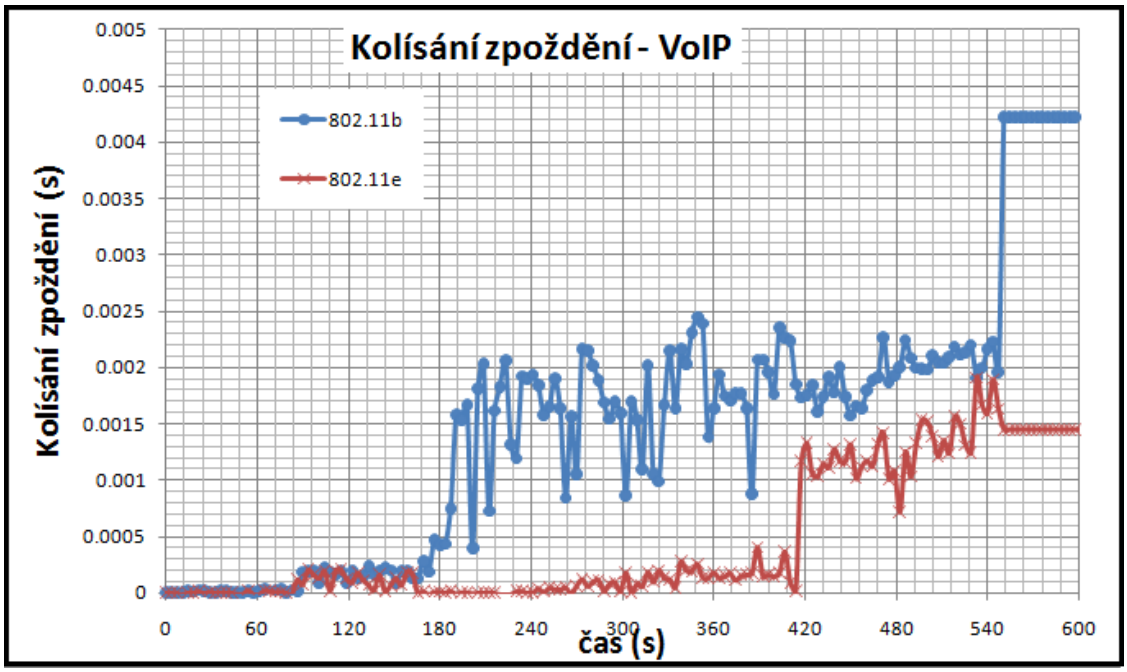
Při zvětšené zátěži jsou maximální hodnoty okolo 100 ms pro 802.11b a 55 ms v síti s podporou 802.11e. Při zvětšení zátěže se hodnoty u zpoždění videa v sítí 802.11e tedy příliš nezměnily. Na rozdíl od sítě 802.11b, kde vzrostly až na 100ms.



Obrázek 6-23 Koncové zpoždění videa v sítích 802.11e a 802.11b

6.4.3.2 Kolísání zpoždění

Kolísání zpoždění chápeme jako rozdíl ve zpoždění doručovaných paketů. Jeho hodnoty se mění v závislosti na zatížení sítě. Pokud nepřesahují 50 ms, jsou ještě vhodné na provoz např. VoIP. S použitím standardu 802.11e se tyto časy minimalizují mechanismem upřednostňováním datových toků nesoucí pakety aplikací citlivých na zpoždění. Vyšší prioritou jim je garantováno rychlejší vyslání a snížení času čekání ve frontě. Na Obrázku 6-24 je zobrazeno kolísání zpoždění v sítích o vyšším zatížení. Naměřené hodnoty kolísání zpoždění jsou vhodné pro kvalitní VoIP hovor.



Obrázek 6-24 Kolísání zpoždění v obou sítích 802.11e a 802.11b

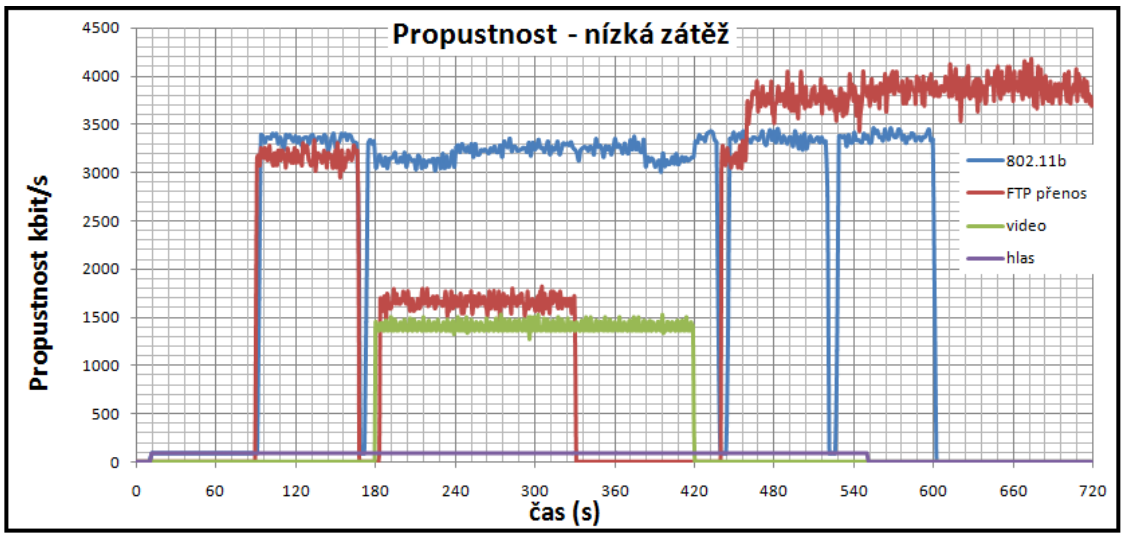
6.4.3.3 Propustnost na směrovači AP A

Propustností označujeme objem dat úspěšně přenesených za jednotku času. Při zvýšené zátěži se propustnost dat s vysokou prioritou nezmění, jak je vidět z Tabulky 6-9. [15]

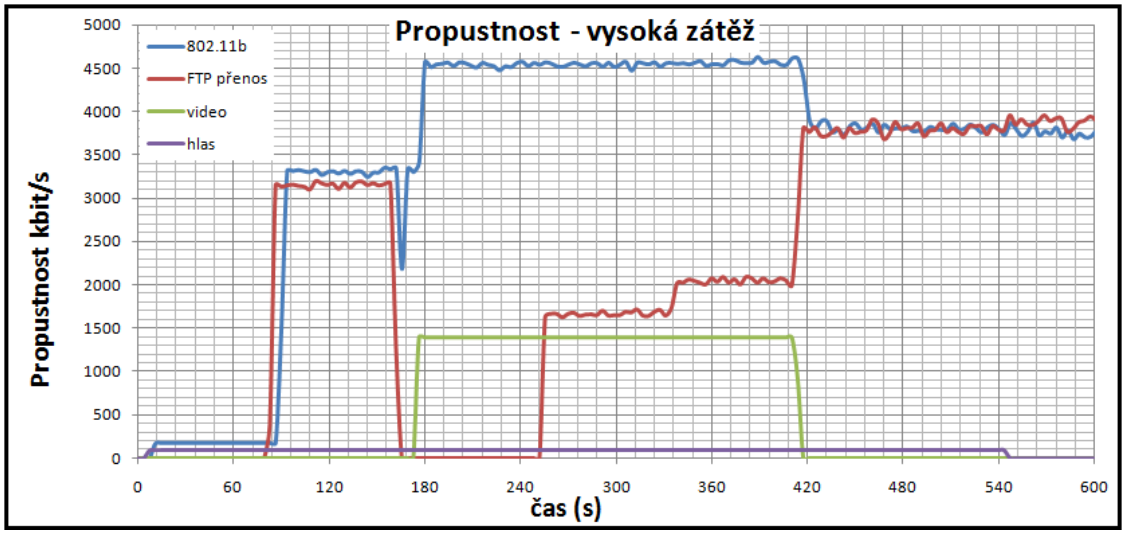
Zátěž	802.11b [kbit/s]	802.11e		
		video [kbit/s]	hlas [kbit/s]	FTP přenos [kbit/s]
nízká zátěž	2718,2	1398,9	95,6	2147
vysoká zátěž	3452,4	1391,7	95,8	2353,4

Tabulka 6-9 Propustnost dat v simulované síti (průměrné hodnoty)

Na Obrázcích 6-25 a 6-26 jsou zobrazeny průběhy měnících se propustností v obou sítích. V síti 802.11b nejsou jednotlivé druhy provozu rozeznávány, a tak je na obrázcích znázorněn jen jeden průběh. U sítě 802.11e jsou zobrazeny propustnosti všech priorit. Průběhy s provozem o vyšších prioritách jako je hlas nebo video zůstávají i při zvyšujícím se provozu neměnné.



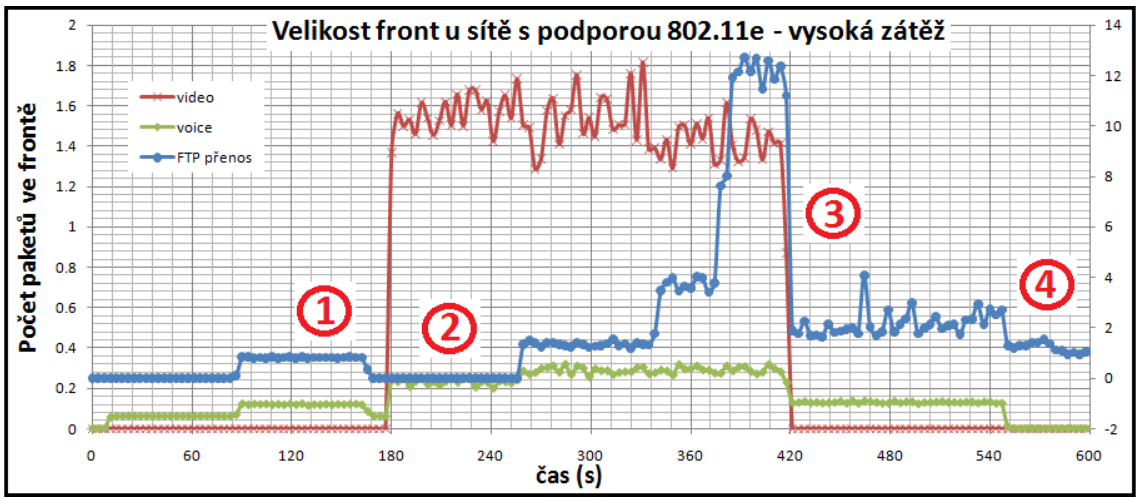
Obrázek 6-25 Propustnost 802.11 – nízká zátěž



Obrázek 6-26 Propustnost 802.11- vysoká zátěž

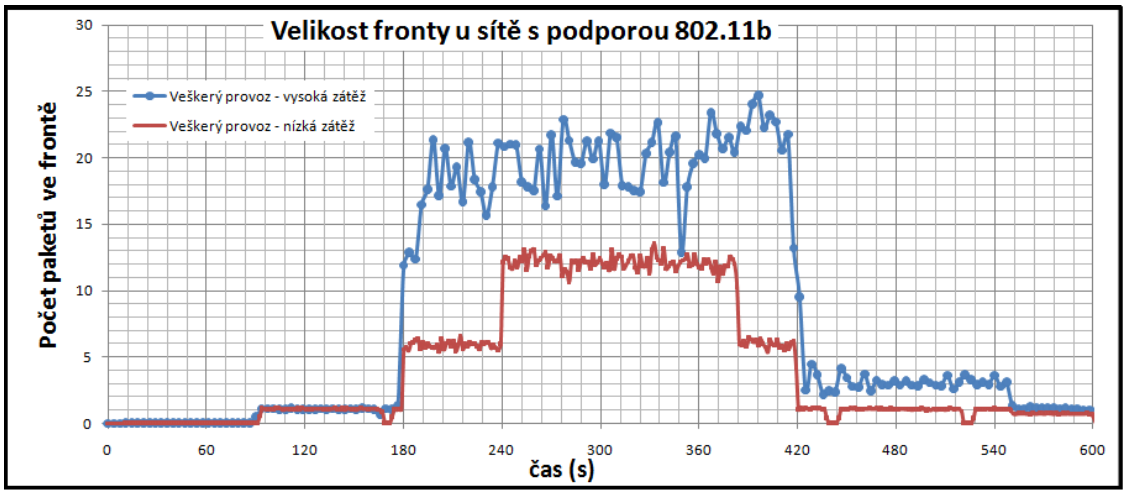
6.4.3.4 Velikost front

Velikost fronty určuje, kolik paketů je v jednotlivých frontách různých priorit – 802.11e nebo jen v jedné frontě – 802.11b a čeká na možnost vyslání. V prvním jmenovaném standardu mají pakety ve frontách přiřazeny různě dlouhé čekací doby, závisející na příslušné třídě přístupu. Hlasu patří nejvyšší priorita, a tak mu náleží nejnižší čekací doby a nejmenší velikost okna soutěžení. Jeho fronta by měla být co nejmenší, aby zdržení vlivem čekání bylo minimální (viz Obrázek 6-27). Počet paketů ve frontě hlasu je nejnižší. Nezvýší se při zatížení FTP přenosem – bod 1 (má nižší prioritu – *best effort* BE). Ovšem při provozu s vyšší prioritou (VI) se o něco málo zvětší. Tato hodnota se zvýší na 0,3 – bod 2. U bodu 3 je vidět rozdíl mezi velikostí fronty videa a FTP přenosu při maximální zátěži. Velikost fronty BE dosahuje čísla 12, zatímco video má počet paketů ve frontě maximálně 1,8. Končí zde také přenos videa, a tak se počet paketů ve frontě hlasu sníží na svou původní úroveň, která byla na začátku – bod 4.



Obrázek 6-27 Velikost fronty u sítě s podporou 802.11e

V síti 802.11b je podpora jen jedné fronty pro všechen provoz. Jednotlivé druhy provozu nejsou nikterak upřednostňovány a dělí se o celé pásmo rovným dílem (viz Obrázek 6-28).

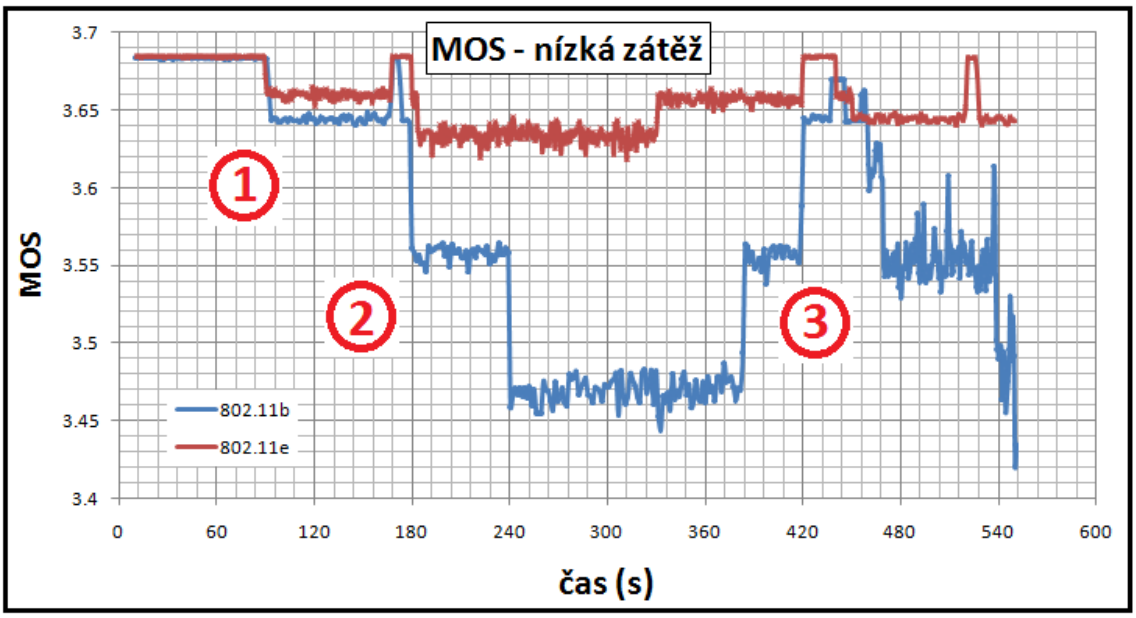


Obrázek 6-28 Velikost jedné fronty v síti 802.11b

6.4.3.5 Kvalita VoIP hovoru

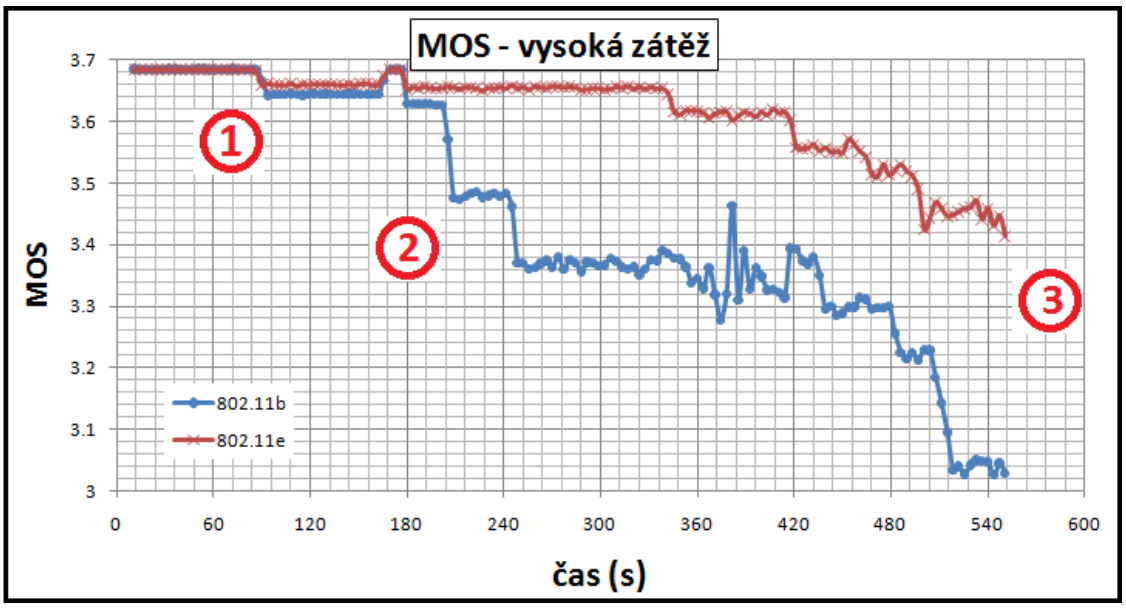
Tento test byl zaměřen na ohodnocení kvality hovoru v síti pomocí parametru MOS. Jeho hodnoty jsou jako známky ve škole, jen v obráceném pořadí. Hodnota 5 udává vynikající kvalitu hovoru srovnatelnou s hovorem mezi lidmi v blízké vzdálenosti. U hodnoty 4 se objevuje mírné rušení. Hovor je ale stále kvalitní i přes zmíněné rušení a je ho možno přirovnat k hovoru v klasické pevné síti. Hodnota 3 značí průměrnou kvalitu, kde je již rušení vnímáno. Pokud bychom začali druhé straně špatně rozumět a rušení by se zvýšilo, je hodnocení rovno 2. Posledním stupněm je hodnota 1. Zde již není možno vést komunikaci. Reálně je v telefonních sítích dosahováno maximálně hodnoty 3,5 až 4,5. [15]

Na následujícím grafu (Obrázek 6-29) je zobrazen průběh měřeného parametru MOS v málo zatížené síti. V síti bez rozlišování provozu je viditelný každý pokles MOS při zapnutí dalšího provozu – bod 1 a 3 FTP a bod 2 vysílání vida. Naopak ve druhé sítí, kde má hlas největší prioritu, nejsou tyto poklesy tak viditelné. Hodnoty MOS se udržují kolem čísla 3,65, které zaručuje dobrou kvalitu hovoru.



Obrázek 6-29 Kvalita MOS v sítích 802.11e a 802.11g – nízká zátěž

Po zvětšení zátěže byly změny v MOS znatelnější. Na začátku je průběh podobný jako na předcházejícím obrázku – bod 1 a 2. MOS se vlivem větší zátěže nejvíce projevil ke konci testu – bod 3. Zde u sítě 802.11e klesl parametr MOS na hodnotu 3,4, která je srovnatelná s hovorem v síti GSM. U druhé sítě klesl MOS k číslu 3.



Obrázek 6-30 Kvalita MOS v sítích 802.11e a 802.11g – vysoká zátěž

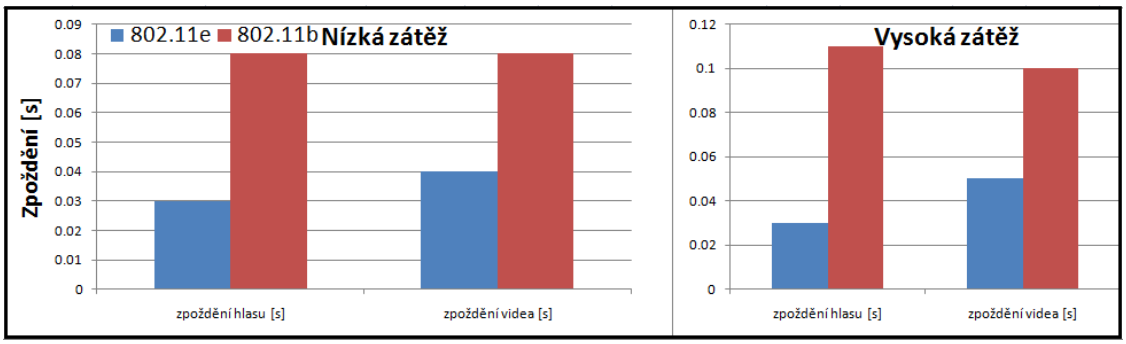
6.4.3.6 Celkové shrnutí měřených parametrů

V sítí se zapnutou podporou standardu 802.11e byly hodnoty měřených parametrů lepší než v sítí bez jeho podpory, jak je vidět z následující tabulky.

Parametr	802.11b		802.11e					
			nízká zátěž			vysoká zátěž		
	nízká zátěž	vysoká zátěž	hlas	video	FTP	hlas	video	FTP
Zpoždění [s]	0.08 hlas 0.08 video	0.11 hlas 0.10 video	0.03	0.04	-	0.03	0.05	-
Propustnost [kbit/s]	2718,2	3512,4	71,8	466,2	2147	71,9	466,7	2353,4
Velikost fronty [počet paketů]	14	25	0.28	1.8	6,1	0.3	1.8	12.7
MOS	3.5	3.4	3,66	-	-	3.62	-	-

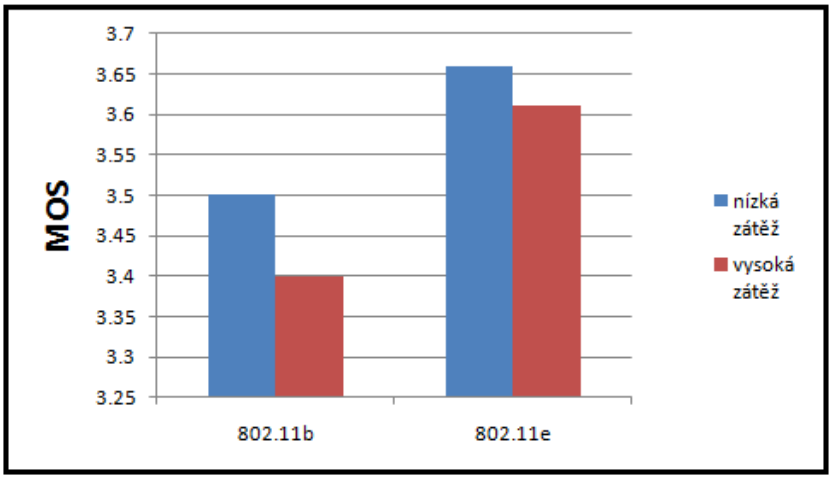
Tabulka 6-10 Porovnání naměřených průměrných hodnot

Graf na Obrázku 6-31 ukazuje vliv zlepšení parametru zpoždění u hlasu a videa v sítí při zapnutí podpory 802.11e.



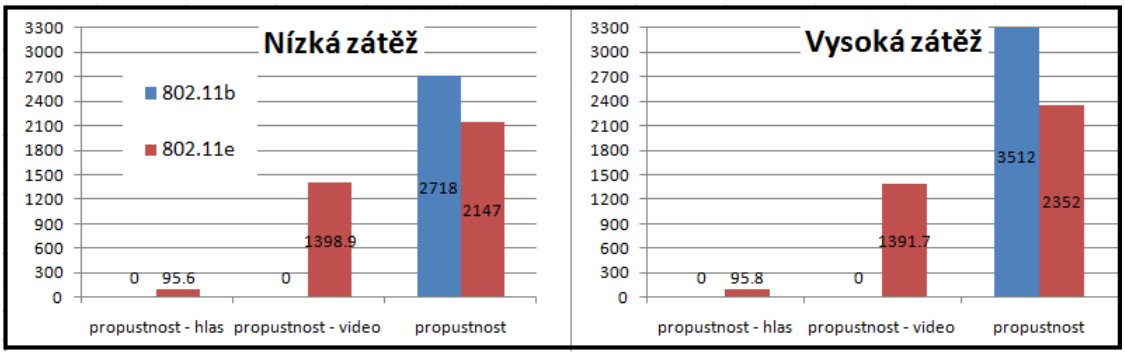
Obrázek 6-31 Srovnání velikosti zpoždění v obou sítích

V následujícím grafu (Obrázek 6-32) je zobrazena průměrná hodnota parametru MOS v síti s podporou 802.11e a v síti bez této podpory. V síti s podporou 802.11e se hodnoty pohybují okolo 3,64 při nízké i vysoké zátěži. V druhé síti hodnoty klesly až na 3,4 při vysoké zátěži.



Obrázek 6-32 Srovnání parametru MOS v obou sítích

V grafu na Obrázku 6-33 jsou znázorněny hodnoty propustnosti v obou sítích. Jak lze vidět tak hodnoty propustnosti u hlasu nebo videa zůstávají díky své vysoké prioritě na stejných hodnotách.



Obrázek 6-33 Srovnání parametru propustnosti v obou sítích

Závěr

V roce 1999, kdy vznikl standard 802.11, slovo WiFi téměř nikdo neznal. Dnes je situace zcela jiná. WiFi sítě jsou především u nás nejdostupnější cestou jak se připojit k internetu. S jejich rostoucí popularitou a vývojem multimediálních služeb se však objevují problémy. Jedná se například o bezpečnost, rychlost, možnost poskytnou aplikacím určitou šířku pásma a garantovat hodnoty zpoždění a další. Problémy s bezpečností se podařilo vyřešit vytvořením mechanismu WPA2, který je dnes jako jediný z běžně používaných mechanismů bezpečný. Rychlost bezdrátových sítí už dnes také není tak závažným problémem. Se vznikem standardu 802.11n je možno dosáhnout až rychlosti 200 Mbit/s. Ale ani takto vysoká rychlost neřeší problém uživatele, který si bude chtít zatelefonovat přes internet v momentě, kdy je síť zatížena dalšími uživateli stahujícími různá data. Síť totiž není schopna rozlišit probíhající provoz a zajistit mu tak určitou garanci parametrů kvality služeb. Proto byl vytvořen standard 802.11e. Ještě než se objevil, vznikla služba WMM s podporou několika jeho funkcí.

Standardu 802.11e a službě WMM je věnována velká část této práce. Bakalářská práce popisuje mechanismy, které jsou využívány při rozlišování provozu a zajišťující různé zacházení s tímto provozem. V závěru je prokázán jejich vliv na reálný provoz v menší bezdrátové síti. Všechny měřené parametry, jako je zpoždění, kolísání zpoždění a ztrátovost, se při zapnutí služby WMM zmenšily. VoIP hovor, který byl při každém testu proveden, ukazoval, jak velký vliv má služba WMM na jeho provoz. Při vypnuté službě WMM v zatížené síti byl hovor v nepřijatelné kvalitě. Situace se zlepšila s jejím zapnutím. Provoz v síti s nižší prioritou byl omezen a na základě toho byl VoIP hovor bezproblémový.

Na závěr byla navrhnuta síť v simulačním programu Opnet Modeler. I přes počáteční nesnáze a problémy, které se vyskytly při návrhu, byla síť dokončena a otestována. Výsledné grafy potvrdily převážnou většinu výsledků z reálného měření. Služby na zajištění QoS fungovaly a poskytly tak službám citlivým na zpoždění potřebné parametry, s kterými byl jejich provoz na vynikající úrovni.

Seznam použité literatury

[1] ENGINEERS, INSTITUTE OF ELECTRICAL AND ELECTRONICS. 2007. *IEEE Std 802.11™-2007.* [Online] 2007. Dostupný z: <http://standards.ieee.org/getieee802/802.11.html. ISBN 0-7381-5656-6>.

[2] ENGINEERS, INSTITUTE OF ELECTRICAL AND ELECTRONICS. 2005. *IEEE Std 802.11e™-2005.* [Online] 2005. Dostupný z: <http:// standards.ieee.org/getieee802/802.11.html. ISBN 0-7381-5656-6>.

[3] GAST, M. 2005. *802.11® Wireless Networks The Definitive Guide.* New York : O'Reilly, 2005. ISBN 0-596-10052-3.

[4] GEIER, J. 2002. *802.11 Beacons Revealed.* [Online] 2002. Dostupný z: < http://www.wi-fiplanet.com/tutorials/article.php/1492071>.

[5] KLAŠKA, L. 2009. *Svět sítí.* archiv článků ohledně problematiky sítí; [Online] 2009. Dostupný z: < http://www.svetsiti.cz>.

[6] KLÍMEK, J. 2008/2009. *Moderní síťová řešení*. [Online] 2008/2009. Dostupný z: < http://www.mff.cuni.cz/>.

[7] MANGOLD, S. 2003. *Analysis of IEEE 802.11e for QoS support in wireless lans.*[Online] 2003. Dostupný z : <http://morse.colorado.edu/~tlen5520/Papers/Mangold80211e.pdf. 1536-1284/03>.

[8] MANGOLD, S. 2006. *IEEE 802.11e Wireless LAN for Quality of Service*. RWTH Aachen Universtity of Technology. [Online] 2006. Dostupný z: <http://www2.ing.unipi.it/ew2002/proceedings/H2006.pdf>.

[9] MOLNÁR K., ZEMAN O., SKOŘEPA M. 2008. *Moderní síťové technologie – laboratorní cvičení, revize 2.* místo neznámé : VUT Brno, 2008.

[10] MOLNÁR, K. 2009. *Bezdrátové síťové technologie I. II. III.* Brno : VUT Brno, 2009. přednášky.

[11] MOLNÁR, K.. 2009. *Zajištění kvality služeb v bezdrátových a mobilních sítích I. a II.* Brno : VUT Brno, 2009. přednášky.

[12] NOVOTNÝ V., KOVÁŘ P. 2008. *Přístupové metody bezdrátových sítí.* [Online] 2008. Dostupný z: <http://access.feld.cvut.cz/view.php?cisloclanku=2008100003>.

[13] OPNET, TECHNOLOGIES. *OPNET Modeler Product Documetation Release 14.5.* součást programu OPNET Modeler.

[14] PETERKA, Jiří. archiv článků a přednášek Jiřího Peterky. [Online]. Dostupný z: < http://www.earchiv.cz>.

[15] PUŽMANOVÁ, R. 2005. *Schválena specifikace pro hlas do WiFi.* [Online] 2005. Dostupný z: <http://www.lupa.cz/clanky/schvalena-specifikace-pro-hlas-do-wifi>.

[16] PUŽMANOVÁ, R. 2006. *Moderní komunikační sítě od A do Z 2 aktualizované vydání.* Brno : Computer Press a.s, 2006. ISBN 80-251-1278-0.

[17] ŠAFRÁNEK M., KOCUR Z. 2008. *Fyzická vrstva Wi-Fi.* [Online] 2008. Dostupný z: < http://access.feld.cvut.cz/view.php?cisloclanku=2008050006>.

[18] SHIVENDRA, P. A PEI, L. *Gigabit Wireless Technologies and Standardization.* [Online]. Dostupný z: <http://www.ieee.li/pdf/viewgraphs/ gigabit_wireless_technologies_and_standardization.pdf>.

[19] ŠPIDLA, M. 2009. *Možnosti narušení bezdrátové přístupové sítě.* Brno : VUT Brno Fakulta elektrotechniky a komunikačních technologií, 2009.

[20] TUREK, L. 2007. *802.11n - Cesta za rychlejším Wi-Fi.* [Online] 2007. Dostupný z: <http://8an.praha12.net/talks/80211n.pdf>.

[21] VOZŇÁK M., PUŽMANOVÁ R. 2009. *Kvalita VoIP souvisí se zabezpečením hovorů.* [Online] 2009. Dostupný z: <http://www.cesnet.cz/sdruzeni/napsali-onas/2009/04/20090415 _Professional_Computing.html>.

[22] WI-FI ALLIANCE. 2004. *Wi-Fi CERTIFIED™ for WMM™ - Support for Multimedia Applications*. [Online] 2004. Dostupný z: <http://www.wi-fi.org/files/wp_1_WMM%20QoS%20In%20Wi-Fi_9-1-04.pdf>.

[23] ZANDL, P. 2003. *WiFi Praktický průvodce.* Brno : Computer Press a.s., 2003. ISBN 80-7226-632-2.

Seznam použitých zkratek

AC	*Access Category*
ACI	*Access Category Index*
ACK	*Acknowledge*
AES	*Advanced Encryption Standard*
AIFS	*Arbitration Interframe Space*
AP	*Access Point*
APSD	*Automatic Power Save Delivery*
BA	*Block Acknowledgements*
BPSK	*Binary Phase Shift Keying*
BSS	*Basic Service Set*
CAP	*Controlled Access Phase*
CCA	*Clear Channel Assessment*
CCK	*Complementary Code Keying*
CCMP	*Counter Mode with Cipher Block Chaining Message Authentication Code*
CFP	*Contention-Free Period*
CP	*Contention Period*
CRC	*Cyclic Redundancy Check*
CSMA/CA	*Carrier Sense Multiple Access/Collision Avoidance*
CTS	*Clear to send*
CW	*Contention Window*
DBPSK	*Differential Binary Phase Shift Keying*
DCF	*Distributed Coordination Function*
DFS	*Dynamic Frequency Selection*
DHCP	*Dynamic Host Configuration Protocol*
DiffServ	*Differentiated Services*
DIFS	*DCF InterFrame Space*
DS	*Distribution system*
DSCP	*Differentiated Services Code Point*
DSSS	*Direct Sequence Spread Spectrum (HR – High Rate)*
DQPSK	*Differential Quadrature Phase-Shift Keying*
EAP	*Extensible Authentication Protocol*
EOSP	*End Of Service Pole*
EDCA	*Enhanced Distributed Channel Access*
EDCF	*Enhanced Distributed Coordination Function*
ESS	*Extended Service Set*
ETSI	*European Telecommunication Standards Institute*
FCS	*Frame Check Sequence*
FSO	*Fiber Space Optics*
FHSS	*Frequency Hopping Spread Spectrum*
GSM	*Global System for Mobile communications*

HC	*Hybrid Coordinator*
HCCA	*HCF Controlled Channel Access*
HCF	*Hybrid Coordination Function*
HiPerLan	*High Performance LAN*
HTTP	*Hypertext Transfer Protocol*
IAPP	*Inter - Access Point Protocol*
IBSS	*Independent Basic Service Set*
IEEE	*Institute of Electrical and Electronics Engineers*
IFS	*InterFrame Space*
IV	*Initialization Vector*
ISS	*Independent Service Set*
LAN	*Local Area Network*
LLC	*Logical Link Control*
MAC	*Media Access Control*
MIC	*Message Integrity Check*
MIP	*Mobile IP*
MIMO	*Multiple Input Multiple Output*
MOS	*Mean Opinion Score*
MSDU	*MAC Service Data Unit*
NAT	*Network address translation*
NAV	*Network Allocation Vector*
OFDM	*Orthogonal Frequency Division Multiplex*
PCF	*Point Coordination Function*
PIFS	*Point Coordination Function Interframe Space*
PLCP	*Physical Layer Convergence Procedure*
PMD	*Physical Medium Dependent*
PPDU	*Physical Layer Service Data Unit*
PSK	*Pre-Shared Key*
PSP	*Power Save Polling*
Pwr. mgt.	*Power Management*
QAM	*Quadrature amplitude modulation*
QAP	*Quality of service supporting Access Point*
QBSS	*QoS supporting Basic Service Set*
QoS	*Quality of Service*
QSTA	*QoS supporting Station*
RA	*Receiving Station Address*
RTS	*Request To Send*
SIFS	*Short InterFrame Space*
SFD	*Start Frame Delimiter*
SSID	*Service Set Identifier*
TA	*Transmitting Station Address*

TID	***T****raffic Identifier*
TIM	*Traffic Indication Map*
TPC	*Transmit Power Control*
TKIP	*Temporal Key Integrity Protocol*
ToS	*Type Of Service*
TSPEC	*Traffic Specification*
TXOP	*Transmission Opportunity*
UP	*User Priorities*
VoIP	*Voice over IP*
WDS	*Wireless Distribution System*
WEP	*Wireless Encryption Privacy*
Wi - Fi	*Wireless Fidelity*
WLAN	*Wireless Local Area Network*
WME	*Wireless Media Extension*
WMM	*Wireless Multi Media*
WMM-SA	*Wireless Multi Media Scheduled Access*
WPA	*WiFi Protected Access*
XOR	*eXclusive OR*

PŘÍLOHA 1: Výstupy z programu Wireshark

Beacon rámec

```
IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
    Frame Control: 0x0080 (Normal)
        Version: 0
        Type: Management frame (0)
        Subtype: 8
        Flags: 0x0
    Duration: 0
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: BelkinIn_ce:4d:34 (00:1c:df:ce:4d:34)
    BSS Id: BelkinIn_ce:4d:34 (00:1c:df:ce:4d:34)
    Fragment number: 0
    Sequence number: 986
IEEE 802.11 wireless LAN management frame
    Fixed parameters (12 bytes)
        Timestamp: 0x0000000D8F9E6183
        Beacon Interval: 0,102400 [Seconds]
        Capability Information: 0x0411
            .... .... .... ...1 = ESS capabilities: Transmitter is an AP
            .... .... .... ..0. = IBSS status: Transmitter belongs to a BSS
            .... ..0. .... 00.. = CFP participation capabilities: No point
                                  coordinator at AP (0x0000)
            .... .... ...1 .... = Privacy: AP/STA can support WEP
            .... .... ..0. .... = Short Preamble: Short preamble not allowed
            .... .... .0.. .... = PBCC: PBCC modulation not allowed
            .... .... 0... .... = Channel Agility: Channel agility not in use
            .... ...0 .... .... = Spectrum Management:
                                  dot11SpectrumManagementRequired FALSE
            .... .1.. .... .... = Short Slot Time: Short slot time in use
            .... 0... .... .... = Automatic Power Save Delivery: apsd not implemented
            ..0. .... .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
            .0.. .... .... .... = Delayed Block Ack: delayed block ack not
                                  implemented
            0... .... .... .... = Immediate Block Ack: immediate block ack not
                                  implemented
    Tagged parameters (94 bytes)
        SSID parameter set: "Svornosti_14"
            Tag Number: 0 (SSID parameter set)
            Tag length: 12
            Tag interpretation: Svornosti_14
        Supported Rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 18,0 24,0 36,0 54,0
            Tag Number: 1 (Supported Rates)
            Tag length: 8
            Tag interpretation: Supported rates: 1,0(B) 2,0(B) 5,5(B) 11,0(B) 18,0
                                                 24,0 36,0 54,0  [Mbit/sec]
        DS Parameter set: Current Channel: 1
        Traffic Indication Map (TIM): DTIM 0 of 1 bitmap empty
            Tag Number: 5 (Traffic Indication Map (TIM))
```

```
            TIM length: 4
            DTIM count: 0
            DTIM period: 1
            Bitmap Control: 0x00 (mcast:0, bitmap offset 0)
        ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
            Tag Number: 42 (ERP Information)
            Tag length: 1
            Tag interpretation: ERP info: 0x0 (no Non-ERP STAs, do not use
                                protection, short or long preambles)
        RSN Information
        Extended Supported Rates: 6,0 9,0 12,0 48,0
            Tag Number: 50 (Extended Supported Rates)
            Tag length: 4
            Tag interpretation: Supported rates: 6,0 9,0 12,0 48,0  [Mbit/sec]
        Vendor Specific: WPS
            Tag Number: 221 (Vendor Specific)
            Tag length: 14
            Version: 0x10
            Wifi Protected Setup State: Configured (0x02)
```

Datový rámec

```
IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x20)
    Frame Control: 0x4208 (Normal)
        Version: 0
        Type: Data frame (2)
        Subtype: 0
        Flags: 0x42
            .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1)
                        (0x02)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .1.. .... = Protected flag: Data is protected
            0... .... = Order flag: Not strictly ordered
    Duration: 0
    Destination address: IPv6mcast_00:01:00:02 (33:33:00:01:00:02)
    BSS Id: AsustekC_b3:5d:7a (00:24:8c:b3:5d:7a)
    Source address: 00:4f:74:30:ad:58 (00:4f:74:30:ad:58)
    Fragment number: 0
    Sequence number: 3484
    CCMP parameters
        CCMP Ext. Initialization Vector: 0x000000001B91
        Key Index: 1
Data (149 bytes)
```

PŘÍLOHA 2 Obrázky z realizace sítě

Budova A

Budova B

Použité vybavení